Andreas Hein

ABZOCKE IM INTERNET? NICHT MIT MIR!

SCHNELLEINSTIEG SICHER SURFEN IM WEB

160 SEITEN

ZEIGEN SIE POTENZIELLEN BETRÜGERN, WER AUF IHREM RECHNER DAS SAGEN HAT

FRANZIS

Andreas Hein

Schnelleinstieg
Sicher surfen im Web

Andreas Hein

SCHNELLEINSTIEG SICHER SURFEN IM WEB

FRANZIS

Bibliografische Information der Deutschen Bibliothek

Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte Daten sind im Internet über http://dnb.ddb.de abrufbar.

Herausgeber: Ulrich Dorn
Layout & Satz: Nelli Ferderer, nelli@ferderer.de
art & design: www.ideehoch2.de
Druck: CPI-Books
Printed in Germany

ISBN 978-3-645-60397-3

INHALT

1 GEFAHREN IM INTERNET

Das Internet ist zu einem ganz selbstverständlichen Teil des Alltags geworden, sodass sich viele Internetnutzer kaum noch ernsthafte Gedanken über die möglichen Gefahren machen, die dort lauern. Umso größer ist jedoch die böse Überraschung, wenn sie Opfer von kriminellen Aktivitäten werden. Weil das Internet längst nicht mehr nur zur Informationsbeschaffung, zum Spielen oder zur Kommunikation genutzt wird, sondern dort auch vermehrt kommerzielle Aktivitäten stattfinden und mit Onlinebanking und Onlineshopping finanzielle Transaktionen abgewickelt werden, wollen sich immer mehr Betrüger auf diesem Wege bereichern.

1.1 Gefahrenlage im Wandel

In den letzten Jahren hat das Sicherheitsbewusstsein bei vielen Internetnutzern überraschenderweise abgenommen, was auch darauf zurückzuführen ist, dass große, spektakuläre Angriffswellen durch Schadprogramme nicht mehr so häufig vorkommen und bekannt werden. Computerviren und Würmer, die weltweit Millionen von PCs befallen und lahmlegen, wie es Melissa und dem I-Love-You-Virus (auch Loveletter genannt) vor 15 Jahren gelang, gibt es heute nicht mehr. Das darf jedoch keineswegs als Entwarnung verstanden werden – ganz im Gegenteil! Es gibt neue Gefahren, die sogar noch gravierendere Folgen haben können.

Moderne Betriebssysteme und Rechner sind zwar tendenziell sicherer geworden, aber es gibt immer noch zahlreiche Schwachstellen, durch die sich Schadprogramme einschleichen können. Doch anders als vor 10 oder 15 Jahren zielen sie zumeist nicht mehr auf eine einfache Sabotage der Rechner oder haben das Ziel, undifferenziert möglichst viele PCs lahmzulegen. Perfiderweise versuchen viele neue Schädlinge, möglichst lange unentdeckt zu bleiben, um so ihren eigentlichen Zweck zu erfüllen. Sie spionieren den Nutzer und dessen Daten aus, um sich später beispielsweise beim Onlinebanking auf Kosten des Opfers zu bereichern, den Rechner fernzusteuern oder andere Manipulationen vorzunehmen. Die Betroffenen werden dabei direkt oder indirekt geschädigt, häufig werden auch ganz konkrete finanzielle Schäden angerichtet.

Handfeste Ziele

Die Amateurhacker der früheren Jahre entwickelten Computerviren, um damit ihr »Können« zu beweisen und ihre Fähigkeiten öffentlich zur Schau zu stellen. Heute werden Schadprogramme professionell entwickelt, und die Computer- und Internetkriminalität ist längst zu einem milliardenschweren Bereich der organisierten Kriminalität geworden.

Mit der neuen Schadsoftware verfolgen Angreifer ganz handfeste Ziele. Bei Angriffen auf Unternehmen werden Daten ausspioniert oder Rechner gezielt sabotiert. Werden Privatanwender nicht direkt finanziell geschädigt, missbrauchen Angreifer deren Rechnerressourcen für ihre Zwecke, indem sie die Kontrolle über die PCs übernehmen und diese fernsteuern. Von den folgenden Schadprogrammen und Angriffszenarien gehen derzeit die größten Gefahren aus.

Ransomware

Als Ransomware bezeichnet man Schadprogramme, die auf dem infizierten Rechner gezielt Dateien verschlüsseln, sodass kein Zugriff darauf mehr möglich ist. Erst nach Zahlung eines Lösegelds versprechen die Angreifer die Übersendung eines Freigabecodes, mit dem die Verschlüsselung wieder aufgehoben werden kann. Manchmal macht Ransomware die Nutzung eines PCs auch komplett unmöglich. Nach dem Einschalten des Rechners erscheint nur noch der Hinweis auf die Sperrung sowie eine Anleitung zur Zahlung des Lösegelds.

DER ERPRESSUNG NACHZUGEBEN BRINGT NICHTS

Wer der Erpressung nachgibt, wird nach der Zahlung des Lösegelds meist bitter enttäuscht, da das versprochene Passwort oder Tool zum Entschlüsseln des Rechners nicht geliefert wird. Der Schaden lässt sich trotz Zahlung nicht beheben. Manchmal bluffen die Erpresser aber auch nur, und die Blockade lässt sich mit ein paar Befehlen leicht aufheben. Tipps und Lösungen zu Ransomware-Angriffen finden Sie im Internet, das Sie dann mit einem nicht infizierten Rechner nutzen müssen.

Ein prominentes Beispiel für Ransomware ist der BKA-Trojaner. Dieser tarnt sich als Mitteilung der Bundespolizei und behauptet, dass auf dem Rechner verbotenes Material entdeckt worden sei. Es erscheint eine entsprechende Mitteilung mit der Aufforderung, einen bestimmten Betrag als Strafzahlung zu leisten.

Um der Forderung Nachdruck zu verleihen, wird der Rechner eingefroren und kann zunächst nicht weiter genutzt werden.

Der BKA-Trojaner war so erfolgreich, dass es mittlerweile zahlreiche Varianten davon gibt. Dieser Schädling kann zwar mit recht einfachen Mitteln deaktiviert werden, sodass eine normale Nutzung des Rechners schnell wieder möglich ist, es gibt aber auch deutlich gefährlichere Ransomware, die sich nicht so leicht abschalten lässt, sodass verschlüsselte Dateien nicht mehr zugänglich sind oder der Rechner nur durch eine komplette Neuinstallation des Betriebssystems wieder nutzbar wird.

Ransomware kommt immer öfter zum Einsatz.

Botnetze und Zombie-Rechner

Zu einem Missbrauch, von dem die Opfer häufig gar nichts oder nur indirekt etwas mitbekommen, kommt es, wenn Rechner durch eine Fernsteuerungssoftware befallen werden. Angreifer bekommen dadurch die Möglichkeit, den Rechner und seine Ressourcen für ihre Zwecke zu verwenden, indem sie einfach entsprechende Befehle übermitteln. Die manipulierten Rechner werden als Zombie-PCs oder einfach als Zombies bezeichnet. Besonders erfolgreiche

Schädlinge dieser Art haben weltweit Millionen von PCs befallen, die wie ein Heer willenloser Sklaven die Befehle ihrer Herren ausführen. Eine solche Ansammlung ferngesteuerter Rechner wird Botnet (oder eingedeutscht Botnetz) genannt.

Ist ein solches Botnetz eingerichtet, nutzen die Betreiber es meistens nicht selbst, sondern vermieten die enormen Ressourcen an andere Interessenten. Häufig wird über diese Netze unerwünschte E-Mail-Werbung (Spam) versendet. Die Rechner werden aber auch missbraucht, um sogenannte DDOS-Angriffe (*Distributed Denial Of Service*) auf Internetserver durchzuführen, die durch massenhafte gleichzeitige Aufrufe durch die ferngesteuerten PCs gezielt überlastet und für andere Besucher unerreichbar gemacht werden. Mit DDOS-Angriffen werden Webshops und andere kommerzielle Internetanbieter bedroht, die durch das Lahmlegen ihrer Server erhebliche Einbußen hätten. Oft kommen zunächst nur kurze Angriffe, um anschließend Schutzgelder von den Betreibern zu erpressen, die häufig lieber zahlen, als weitere Attacken dieser Art hinzunehmen oder teure Schutzvorkehrungen zu installieren.

Als Besitzer eines PCs, der durch eine Schadsoftware infiziert und Teil eines Botnetzes ist, bekommen Sie jedoch meist nicht mit, dass Ihr Rechner für derartige Machenschaften missbraucht wird, und sind völlig ahnungslos. Einige Provider informieren daher ihre Kunden, wenn sie verdächtige Aktivitäten an deren Internetzugängen feststellen.

HILFE BEIM BOTNET-BERATUNGSZENTRUM

Haben Sie den Verdacht, dass Ihr Rechner Teil eines Botnetzes ist, können Sie sich auf der Website des Anti-Botnet-Beratungszentrums darüber informieren, wie Sie diese Schadsoftware wieder entfernen und sich vor derartigen Übergriffen künftig schützen können. Die Seite erreichen Sie unter der Adresse *www.botfrei.de*.

Betrügereien beim Onlinebanking

Besonders im Fokus der Betrüger stehen natürlich Anwender, die ihre Geldgeschäfte via Onlinebanking tätigen, denn hier machen sich Betrügereien direkt in klingender Münze bezahlt. Bereits seit geraumer Zeit findet ein Wettlauf

zwischen Anbietern und Betrügern statt. Auf verbesserte Sicherheitsmaßnahmen der Banken reagieren Angreifer schnell mit neuen Schadprogrammen, die angepasst wurden, um die neuen Schutzmechanismen auszuhebeln.

Das Abfragen von TANs gehörte zu den ersten Phishing-Attacken.

Beim Onlinebanking wird ein zweites Bedrohungspotenzial bei der Internetnutzung offenbar, bei dem Betrüger nicht auf eine Schadsoftware setzen, um an Daten zu gelangen, sondern bei dem Anwender dazu gebracht werden, selbst Daten preiszugeben, die für die Betrügereien verwendet werden. Diese Manipulationsversuche werden Phishing genannt. Am bekanntesten sind Phishing-Varianten, die Opfer dazu verleiten, ihre Bankdaten, wie PINs und Transaktionsnummern (TANs) für das Onlinebanking oder auch Kreditkartendaten mitzuteilen.

Identitätsdiebstahl

Betrügereien beim Onlinebanking stellen eine besonders folgenreiche Variante des Identitätsdiebstahls dar. Unter Identitätsdiebstahl im Internet versteht man alle Attacken, bei denen durch das Ausspionieren persönlicher Daten und anderer geheimer Zugangsdaten (Passwörter, Nutzernamen etc.) Angreifer unter der Identität ihres Opfers im Internet agieren und beispielsweise Geschäfte tätigen. Das eigentliche Ausspähen der Daten passiert zum einen durch das klassische Phishing per E-Mail oder auf manipulierten Webseiten, es gibt aber auch Spionagetools (Spyware), die wie andere Schadprogramme auf die Rechner geschmuggelt werden und gezielt Zugangsdaten und vertrauliche Informationen abfangen.

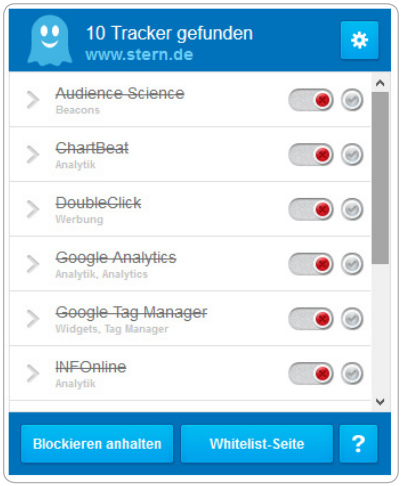
Wie schlimm dieser Identitätsdiebstahl tatsächlich ist, hängt von den Aktivitäten ab. So mag es auf den ersten Blick vielleicht kaum der Rede wert sein, wenn Zugangsdaten für ein Onlineforum in falsche Hände geraten, aber wenn in der Folge illegale Inhalte gepostet werden, kann dies erhebliche Konsequenzen für den Kontoinhaber bedeuten.

AUF DAS E-MAIL-KONTO ACHTEN

Besonders problematisch ist der Zugriff von Dritten auf das E-Mail-Konto, da über den Zugang zum elektronischen Postfach Angreifern zahlreiche weitere Optionen offenstehen. So können in vielen Fällen auch Konten bei anderen Onlinediensten übernommen werden, indem Passwortänderungen bei diesen Diensten über das E-Mail-Konto beantragt werden. Angreifer können sich über das E-Mail-Konto auch einen Zugang zu Konten bei Onlineshops oder Bezahldiensten verschaffen.

Unerwünschte Überwachung und Datenweitergabe

Neben dem Identitätsdiebstahl durch Kriminelle gibt es eine zweite Variante der unerwünschten Weitergabe persönlicher Daten durch die Überwachung von Onlineaktivitäten. Spätestens seit den Snowden-Enthüllungen sollte jeder Internetnutzer wissen, dass die nahezu lückenlosen Überwachungsmöglichkeiten der Geheimdienste keineswegs Hirngespinste verschrobener Verschwörungstheoretiker oder Fantastereien von Hollywood-Regisseuren sind, sondern traurige Realität.



Auf fast allen Webseiten gibt es Tracker und Analysetools.

Doch die Kontrolle der Internetaktivitäten durch Geheimdienste und ähnliche Institutionen ist nur ein Aspekt der Überwachung, auch bei den großen Internetkonzernen werden fleißig Daten gesammelt. Dieses »Tracking« geschieht zwar angeblich nur in anonymisierter Form, doch eine Garantie, dass die Daten nicht doch mit weiteren

persönlichen Informationen zu personenbezogenen Profilen zusammengestellt werden, gibt es nicht. Die Methoden, mit denen Internetsurfer überwacht werden, werden immer komplexer. Auch hier gibt es ein Hase-und-Igel-Wettrennen zwischen den Tracking-Techniken zur Erfassung und Aufzeichnung der Aktivitäten und den Werkzeugen zur Vermeidung dieser Überwachung.

Die Überwachung aller Internetaktivitäten durch Geheimdienste ist ein Problem, das von vielen Anwendern nicht als besonders dramatisch empfunden wird. Häufig ist zu hören, dass man ja sowieso nichts zu verbergen habe und die Überwachung schließlich ein legitimes Instrument im Kampf gegen Kriminalität und Terrorismus sei. Nur eine Minderheit weist dagegen völlig zu Recht darauf hin, dass eine verdachtslose Überwachung aller Bürger durch weitgehend unregulierte Geheimdienste gegen fundamentale Menschen- und Bürgerrechte verstößt und damit beispielsweise auch das Recht auf Privatsphäre ausgehebelt wird. Schutzmaßnahmen, mit denen Sie sich diesen umfassenden Überwachungsaktivitäten entziehen können, sind nur sehr schwer umzusetzen, da diese Organisationen mit hoch effizienten Mitteln arbeiten und es auch keine funktionierenden Ausweichstrategien gibt.

Der ganz normale Betrug

Natürlich gibt es im Internet weitere Gefahren und Betrügereien, die elektronische Gegenstücke zu konventionellen Betrugsmethoden im realen Leben sind. So wird beispielsweise per E-Mail oder in sozialen Netzwerken für dubiose Geldanlagen geworben, oder es wird eine großzügige finanzielle Belohnung in Aussicht gestellt, wenn Adressaten bereit sind, beim Transfer eines vermeintlichen Vermögens aus einem Entwicklungsland zu helfen, wobei sie allerdings einige Kosten im Voraus tragen müssen. Zu den bekanntesten derartigen Betrugsmaschen gehört die »Nigeria-Connection«, deren E-Mails auch nach vielen Jahren immer noch in elektronischen Postfächern zu finden


Lieber Freund,
Ich vermute das diese E-Mail eine Überraschung für Sie
sein wird, aber es ist wahr.
Ich bin bei einer routinen Überprüfung in meiner Bank wo ich arbeite,
auf einem Konto gestoßen, was nicht in anspruch genommen worden ist,
wo derzeit $14.300,000 ((vierzehnmillionendreihundert US
Dollar) gutgeschrieben sind.
Dieses Konto gehörte Herr Christian Eich, der ein Kunde in unsere Bank
war, der leider verstorben ist. Herr Christian Eich war ein gebürtiger
Deutscher.
Damit es mir möglich ist dieses Geld $14.300,000 inanspruch zunehmen,
benötige ich die zusammenarbeit eines Ausländischen Partners wie Sie,
den ich als Verwandter und Erbe des verstorbenen Herr Eich vorstellen kann,
damit wir das Geld inanspruch nehmen können.
Für diese Unterstützung erhalten Sie 30% der Erbschaftsumme und die
restlichen 70%
teile ich mir mit meinen zwei Arbeitskollegen, die mich bei dieser
Transaktion ebenfalls unterstützen.
Wenn Sie interessiert sind, können Sie mir bitte eine E-Mail schicken,

Mit E-Mails wie dieser locken Betrüger ihre Opfer an.

sind. Bei diesen Betrügereien ersetzt das Internet lediglich andere Kommunikationskanäle (Brief, Telefon oder Fax), über die derartige Kontakte früher hergestellt wurden.

Vorsicht beim Onlineshopping

Aufpassen müssen Sie beim Einkaufen im Internet, auch hier lauern Gefahren. Vor allem dann, wenn Waren oder Dienstleistungen im Voraus bezahlt werden, gibt es Risiken. Bei Onlineauktionen ist Vorauszahlung üblich, und die Waren werden normalerweise erst nach Zahlungseingang versendet. Betrüger machen sich dies zunutze, indem sie über gehackte Konten Waren anbieten und dafür kassieren, diese dann aber natürlich nicht liefern. Sie fügen dadurch nicht nur dem Käufer erheblichen Schaden zu, sondern auch dem eigentlichen Kontoinhaber.

In Mode gekommen ist auch der Betrug mit Ferienhäusern, die von unberechtigten Personen zur Miete angeboten werden. Zum direkten finanziellen Schaden kommt noch der zusätzliche Ärger für die Opfer, die an ihrem Urlaubsziel erfahren müssen, dass sie mit dem tatsächlichen Inhaber der Immobilie gar

Die Onlineanmietung von Ferienhäusern kann problematisch sein.

keinen Vertrag und damit auch keine Unterkunft haben. Die Betrüger gehen sehr raffiniert vor und haben in einigen Fällen sogar den E-Mail-Verkehr zwischen Anbietern und Interessenten auf großen und renommierten Ferienwohnungsportalen umgeleitet und manipuliert.

Eine populäre Masche von Abzockern waren Abofallen, bei denen ein unvorsichtiger Klick dazu führte, dass man, ohne es zu wollen, einen Abovertrag abschloss. Nachdem dank der verschärften Gesetzgebung dieser Internetbetrug an Bedeutung verloren hatte, gibt es ähnliche Machenschaften nun im Bereich der mobilen Apps für Smartphones und Tablets.

WAS FÜR GEFAHREN-QUELLEN GIBT ES?	WELCHE MÖGLICHEN AUSWIRKUNGEN HABEN DIE BEDROHUNGEN?	IN WELCHER FORM KÖNNEN SIE MIT DIESEN GEFAHREN IN KONTAKT KOMMEN?
Schadprogramme	Ausspionieren von Daten (auch zum Vorbereiten weiterer Attacken). Missbrauch von Rechnerressourcen (Botnetze zum Spam-Versand, DDOS-Attacken etc.). Erpressung durch Verschlüsselung von Dateien oder Sperre des Rechners. Spezielle Angriffe auf das Onlinebanking. Missbrauch von Smartphones durch teure Sonderrufnummern und Premium-Dienste etc.	Download von Schadsoftware, die sich als harmlose Anwendungen oder Apps tarnen. Automatische Übertragung der Schadsoftware durch Surfen auf manipulierten Webseiten, die derartige Inhalte verteilen. Öffnen von verseuchten E-Mail-Dateianhängen. Öffnen von scheinbar harmlosen, aber verseuchten Dokumenten.
Phishing/ Social Engineering	Ausspionieren von Zugangsdaten wie Passwörtern für Onlinedienste.	Phishing-Mails mit entsprechenden Auskunftsaufforderungen. ▸

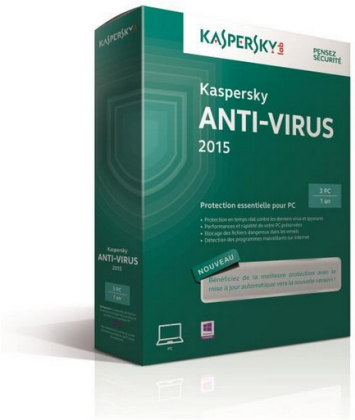
WAS FÜR GEFAHREN-QUELLEN GIBT ES?	WELCHE MÖGLICHEN AUSWIRKUNGEN HABEN DIE BEDROHUNGEN?	IN WELCHER FORM KÖNNEN SIE MIT DIESEN GEFAHREN IN KONTAKT KOMMEN?
Phishing/ Social Engineering	Ausspionieren von Daten für das Onlinebanking oder anderer Finanzdaten. Identitätsdiebstahl/ Übernahme von Konten bei Onlinediensten (E-Mail, soziale Netzwerke, Onlineshops etc.).	Phishing-Webseiten mit entsprechenden Auskunfts-aufforderungen. Links auf Phishing-Webseiten in E-Mails, Chats oder sozialen Netzwerken. Download von Schadsoftware mit Spyware- bzw. Spionage-funktion.
Überwachung/ unerwünschte Datenweitergabe und Daten-sammlung	Abhören vertraulicher Kommunikationsinhalte. Sammeln von Daten zum Erstellen von Nutzerprofilen.	Fehlende oder unzureichende Verschlüsselung. Freiwillige Preisgabe von persönlichen Informationen. Fehlende oder unzureichende Abwehrmaßnahmen gegen-über Datensammlern.
Betrug beim Onlinehandel und sonstige Betrügereien, Abofallen	Finanzielle Verluste durch bezahlte, aber nicht geliefer-te oder minderwertige Wa-ren oder Dienstleistungen. Finanzielle Verluste durch Vorauszahlungen auf in Aussicht gestellte, aber nicht vorhandene Profite. Finanzielle Verluste durch versehentliche Abschlüsse nicht gewollter Abonnements.	Einkaufen von Waren oder Dienstleistungen im Internet. Reagieren auf Kontakt-aufnahme per Mail, Chats etc. Unbedachtes Anklicken von Bestätigungslinks.

1.2 Nur keine Panik

Auch wenn die Aufzählung der potenziellen Gefahren auf den ersten Blick recht abschreckend wirkt, müssen Sie nicht gleich in Panik geraten und auf die Internetnutzung verzichten. Zum Glück gibt es zahlreiche Möglichkeiten, die Risiken so weit zu verringern, dass Sie sich weiterhin weitestgehend unbeschwert im Internet bewegen und von den vielfältigen Nutzungsmöglichkeiten profitieren können.

Antivirensoftware

Zum einen gibt es Hilfsmittel, mit denen Sie sich schützen können, zum anderen können Sie vorsichtig agieren, um den größten Gefahren aus dem Weg zu gehen. Die wichtigste zusätzliche Schutzvorkehrung ist ein aktuelles Antivirenprogramm, das den Computer vor Infektionen durch Schadsoftware schützt. Unverzichtbar ist eine solche Software auf Windows-PCs, also Desktops und Notebooks mit dem Microsoft-Betriebssystem Windows, da die allermeisten Schadprogramme auf diese Rechnervariante spezialisiert sind.



Für Windows-Rechner ist ein Antivirenprogramm unverzichtbar.

Im Bereich der Mobilgeräte, also bei Smartphones und Tablets, ist die Bedrohung durch Schadsoftware nicht ganz so groß.

WENIGER RISIKEN BEI MAC UND LINUX

Deutlich geringer ist das Risiko dagegen für Nutzer von Apple-Computern oder Linux-PCs. Diese Plattformen sind bislang weitgehend von Angriffen verschont geblieben, wobei das weniger auf ein überlegenes Sicherheitskonzept dieser Betriebssysteme zurückzuführen ist, sondern vielmehr daran liegt, dass diese Rechner nur geringe Marktanteile haben. Daher lohnt es sich deutlich weniger, spezielle Schadprogramme dafür zu entwickeln.

Aber auch hier gibt es erhebliche Unterschiede zwischen den verschiedenen Betriebssystemen. So gelten iOS-Geräte (iPhone und iPad) als recht sicher, und auch bei Windows Phone drohen derzeit kaum Gefahren. Dies liegt daran, dass Anwender Apps für diese Geräte ausschließlich über die offiziellen App-Stores von Apple bzw. Microsoft installieren können. Alle Apps, die in den Stores veröffentlicht werden, werden zuvor gründlich geprüft. Bisher konnten verseuchte oder gefährliche Apps meistens erfolgreich herausgefiltert werden. Hinzu kommt, dass Ganoven durch die Prüfungen schon im Vorfeld abgeschreckt werden. Nur sehr wenige bedenkliche Programme konnten diese Hindernisse überwinden.

Anders sieht es dagegen bei Android aus. Hier können Apps auch aus anderen Quellen auf den Geräten installiert werden, sodass ein deutlich höheres Risiko besteht. Daher sollten Sie auf einem Android-Smartphone oder -Tablet immer auch eine Antivirensoftware nutzen. Bei iPhone und iPad ist das nicht notwendig. Auch für Windows Phone-Smartphones benötigen Sie keine Antivirensoftware, während Sie bei Tablets, die mit Windows 8.1 ausgestattet sind, sehr vorsichtig sein müssen. Genau wie bei allen Windows-Versionen für Desktops-PCs und Notebooks ist ein umfassender Schutz auch für Windows-Tablets unbedingt notwendig.

Mit Windows 10, das auf allen Geräten, von Desktop-PC und Notebook über Tablet bis zum Smartphone, zum Einsatz kommen soll, könnte sich das Risiko dann auch bei den Smartphones erhöhen. Genaueres lässt sich dazu derzeit allerdings noch nicht sagen. Windows 10 erscheint im Herbst 2015.

Auf Android-Geräten sollten Sie ebenfalls eine Antivirensoftware verwenden.

Kein hundertprozentiger Schutz

Allerdings dürfen Sie sich auch bei Verwendung eines aktuellen Antivirenprogramms nicht in völliger Sicherheit wiegen. Selbst die beste Software kann keinen perfekten Schutz bieten. Wirklich sicher schützen diese Anwendungen nur gegen Schädlinge, die in den Laboren der Antivirenspezialisten bereits enttarnt wurden. Gelingt es der Malware (Kurzform von *Malicious Software*, also »bösartige Software«), über eine längere Zeit unentdeckt zu bleiben, kann auch das beste Antivirenprogramm keinen vollständigen Schutz bieten.

Besonders »maßgeschneiderte« Schadprogramme, die ganz gezielt nur auf wenigen Rechnern eingeschleust werden, um diese auszuspionieren oder zu

sabotieren, bleiben oft über einen sehr langen Zeitraum unentdeckt. Allerdings richten sich derartige Angriffe meist nicht gegen Privatpersonen, sondern diese Schädlinge werden ganz gezielt in Unternehmen oder andere Organisationen eingeschleust, etwa über das sogenannte Spear-Phishing.

ANTIVIRENPROGRAMM REICHT MEIST AUS

Außer einer Antivirensoftware benötigen Sie normalerweise keine weiteren Schutzprogramme. Personal Firewalls, wie sie früher oft empfohlen wurden, bringen bei modernen Betriebssystemen keinen nennenswerten Zusatznutzen mehr, da diese bereits eine Firewall eingebaut haben. Auch Phishing-Filter, mit denen der Aufruf von Webseiten blockiert wird, die Schadcode verteilen oder auf denen Besucher ausspioniert werden, sind in den meisten Browsern bereits integriert, sodass keine zusätzlichen Programme angeschafft werden müssen. Sinnvoll können dagegen spezielle Browsererweiterungen sein, die die automatische Ausführung potenziell gefährlicher Inhalte blockieren. Derartige Plug-ins gibt es mittlerweile für die meisten populären Webbrowser.

Der Begriff »Antivirenprogramm« für Schutzanwendungen stammt noch aus den Zeiten, als PCs vor allem durch Computerviren bedroht waren. Ein Computervirus ist allerdings nur eine spezielle Art von Schadsoftware, die mittlerweile gar keine große Rolle mehr spielt und von modernen Varianten abgelöst wurde. Einige dieser Malware-Varianten haben Sie hier bereits kennengelernt, wobei die Schädlinge sich meist gar nicht mehr genau in eine der verschiedenen Kategorien einordnen lassen, sondern mehrere Tricks und Schadfunktionen miteinander kombinieren.

Die wichtigsten Begriffe im Zusammenhang von Schadprogrammen sind folgende:

- **Computervirus:** Eigentlich ein Schadprogramm, das die Eigenschaft hat, sich selbstständig zu vervielfältigen, indem es andere Dateien befällt und diese meist auch zerstört. Schon früh wurde der Begriff im allgemeinen Sprachgebrauch für Schadprogramme aller Art verwendet.
- **Computerwurm:** Ein Schadprogramm, das in der Lage ist, sich völlig eigenständig auszubreiten. Es gelangt von einem befallenen Rechner auf einen anderen, indem es beispielsweise Netzwerkverbindungen nutzt.

- **Trojanische Pferde (Trojaner):** Ursprünglich wurde dieser Begriff benutzt, um die Ausbreitungsweise eines Schadprogramms zu beschreiben. In Anlehnung an das antike Vorbild zeichnet sich ein trojanisches Pferd dadurch aus, dass in einem scheinbar nützlichen oder sinnvollen Programm zusätzlich eine gefährliche oder zerstörerische Komponente vorhanden ist. Heutzutage wird die Bezeichnung Trojaner allerdings ähnlich wie Computervirus als Oberbegriff für viele Schädlingsvarianten verwendet.
- **Backdoor:** Ein Schadprogramm, das eine Hintertür (meist in Form von Kommunikationsschnittstellen) auf dem befallenen Rechner öffnet, über die der Angreifer die Kontrolle über den Rechner bekommt und dann beispielsweise weitere Schadprogramme installieren kann.
- **Botnet:** Ein Netzwerk fernsteuerbarer Rechner, die dazu unbemerkt mit einer entsprechenden Schadsoftware modifiziert wurden. Häufig umfassen Botnetze Hunderttausende oder Millionen von Rechnern. Die auf diese Weise ausgenutzten Rechner werden auch »Zombie-PCs« genannt.
- **Spyware:** Oberbegriff für spionierende Software, die Daten sammelt und übermittelt. Spyware kann völlig unerkannt und unbemerkt mittels eines Trojaners oder einer Backdoor auf den Rechner gelangen und beispielsweise durch Aufzeichnung der Tastatureingaben geheime Passwörter abfangen. Als Spyware werden aber auch Programme oder Apps bezeichnet, die das Surfverhalten aufzeichnen und an den Anbieter senden, um daraus Nutzerprofile für passgenaue Werbung zu erstellen.
- **Ransomware:** Ein Schadprogramm, das Dateien verschlüsselt. Damit kann der Zugriff auf Daten verwehrt oder sogar die Nutzung des gesamten Rechners unmöglich gemacht werden. Ein zum Entschlüsseln bzw. Entsperren notwendiges Passwort (oder auch eine Software) versprechen die Betrüger gegen Bezahlung eines Lösegelds zu liefern. Längst nicht immer wird dieses Versprechen tatsächlich eingehalten.
- **Phishing:** Das Ausspionieren von Zugangsdaten und anderen sicherheitsrelevanten Informationen (Passwörter, PINs, TANs, Kreditkartennummern etc.), bei dem die Kontaktaufnahme häufig via E-Mail geschieht. Phishing-Mails werden mittlerweile so gut gemacht, dass sie kaum von seriösen Anfragen zu unterscheiden sind. Auch über entsprechend manipulierte Webseiten wird versucht, Zugangsdaten abzufangen.

- **Spear-Phishing:** Personalisierter, ganz gezielter Phishing-Angriff auf bestimmte Personen. Hier nutzen Angreifer zuvor erworbenes Wissen (etwa zu persönlichen oder beruflichen Situationen), um den Empfänger zur Herausgabe von Daten oder Informationen zu bewegen. Auch Schadsoftware wird auf diesem Weg verbreitet, indem beispielsweise bei einem E-Mail-Empfänger gezielt der Eindruck erweckt wird, dass er eine harmlose Datei von einem ihm bekannten Absender und zu einer aktuellen Thematik erhält, in der sich jedoch ein Schädling versteckt.

1.3 Preis der Sicherheit

Sicherheit beim Surfen hat wie alles andere im Leben seinen Preis. Dieser Preis ist nicht im Sinne einer finanziellen Aufwendung, etwa dem Kaufpreis für ein Antivirenprogramm, zu verstehen, sondern besteht in zusätzlichem Aufwand oder Einschränkungen bei der Internetnutzung. Bei Antivirenprogrammen gibt es neben kostenpflichtigen Produkten auch Gratislösungen, deren Leistungsfähigkeit nicht zwangsläufig schlechter ist.

SICHERHEIT IST EINE DAUERAUFGABE

Sicherheit beim Surfen stellt sich nicht von allein ein. Sie müssen selbst aktiv werden! Dabei ist es nicht mit einer einmaligen Aktion wie der Installation eines Antivirenprogramms getan, sondern Sie sind dauerhaft gefordert, aufmerksam zu bleiben und vorsichtig zu handeln.

Sie müssen damit rechnen, dass Sie zusätzliche Sicherheit mit einem größeren Aufwand oder Komfortverlust erkaufen müssen. Wenn Sie Daten vor der Übertragung beispielsweise verschlüsseln wollen, benötigen Sie nicht nur eine geeignete Software, der Vorgang erfordert auch etwas Zeit und Arbeit. Ähnliches gilt für andere Sicherheitsmaßnahmen bei der Internetnutzung, wie etwa das Überprüfen von Zertifikaten oder die Nutzung von Skriptblockern im Browser, die einerseits zwar Schutz vor unerwünschten Schadprogrammen bieten, andererseits die Nutzbarkeit vieler Webseiten aber stark einschränken.

SICHERHEIT ERFORDERT ZUSÄTZLICHE ANSTRENGUNGEN

Bequemlichkeit kann auch in anderer Hinsicht ein Risiko sein. Wenn Sie beispielsweise jeden Link einfach anklicken, der Ihnen per E-Mail zugeschickt oder auf Facebook oder ähnlichen Diensten von vermeintlichen Bekannten empfohlen wird, dürfen Sie sich nicht wundern, wenn Ihr Rechner infiziert wird. Besonders problematisch ist die Bequemlichkeit allerdings im Hinblick auf Passwörter. Diese stellen bei den meisten Internetdiensten das alleinige Authentifizierungsmerkmal dar, und wenn ein Passwort in die falschen Hände gerät, drohen erhebliche Gefahren. Wenn Sie allerdings vor der Passwortflut kapitulieren und zu einfache Passwörter verwenden und/oder ein- und dasselbe Passwort für viele oder sogar alle Gelegenheiten verwenden, kann das schnell äußerst unangenehme Konsequenzen haben.

Etwas Mühe macht auch das Überprüfen Ihrer Anwendungen und Apps im Hinblick auf Aktualität. Dies ist deshalb so wichtig, weil alte Programmversionen häufig Schwachstellen aufweisen, die von den Herstellern nicht mehr beseitigt werden. Sicherheitslücken in veralteten Programmen werden häufig von Angreifern ausgenutzt, um Schadsoftware auf die Rechner zu schmuggeln. Zwar besitzen viele Anwendungen mittlerweile eine automatische Update-Funktion, es gibt aber noch diverse Programme, bei denen Sie selbst aktiv werden müssen, um die aktuelle Version zu installieren.

Außerdem sollten Sie sich auch aktiv über die aktuellen Bedrohungen und Entwicklungen im Bereich der Computerkriminalität informieren. Die Webseiten der großen Sicherheitsunternehmen und Antivirenspezialisten sind gute Anlaufstellen. Doch nicht nur dort erhalten Sie aktuelle Informationen, auch Einrichtungen wie Verbraucherschutzorganisationen oder Computermagazine informieren Sie über die neuesten Entwicklungen. Je eher Sie über aktuelle Bedrohungen Bescheid wissen, desto schneller können Sie Gegenmaßnahmen einleiten oder Ihr Verhalten anpassen.

Sicherheit durch Verzicht

Sicherheit im Internet setzt nicht nur einen gewissen Aufwand voraus, in einigen Fällen besteht die sicherste Option schlichtweg darin, dass Sie auf bestimmte Angebote oder Dienste verzichten. Besonders relevant ist das im Hinblick auf die Überwachung und Sammlung persönlicher Daten im Internet. Zwar gibt es auch hier verschiedene Möglichkeiten, sich zu schützen, doch in vielen Bereichen können Sie sich im Grunde nicht mehr wehren. Wenn Facebook wieder einmal seine Datenschutzpraxis ändert, um mehr über das Surfverhalten seiner Nutzer zu erfahren, damit anschließend optimierte Werbeannoncen geschaltet werden können, haben Sie keine andere Wahl, als diese Praxis zu akzeptieren oder auf die Facebook-Nutzung komplett zu verzichten.

Auch viele andere Dienste können Sie nur nutzen, wenn Sie persönliche Daten preisgeben. Ortsbezogene Dienste setzen voraus, dass die Anbieter wissen, wo Sie sich gerade befinden. Dieselben Standortdaten, die dazu genutzt werden, Ihnen anzuzeigen, wo sich eine Pizzeria oder ein freier Parkplatz in der Nähe befindet, können natürlich auch dazu verwendet werden, ein Bewegungsprofil zu erstellen. Sie müssen den Anbietern blind vertrauen, wenn diese Ihnen versichern, dass Ihre Standortdaten nur zum gewünschten Zweck verwendet und ausreichend geschützt werden. Sie müssen daher immer abwägen, ob Sie einem Anbieter vertrauen oder besser auf seine Dienste verzichten – es sei denn, Ihnen ist es egal, wer was über Sie weiß und was mit Ihren Daten geschieht.

GESUNDE SKEPSIS HILFT

Gegen viele der Betrugsversuche im Web hilft der gesunde Menschenverstand. Beim Onlineshopping etwa sollten Sie bei vermeintlichen Superschnäppchen trotz aller Verlockungen immer skeptisch bleiben, vor allem wenn es sich um Angebote unbekannter Unternehmen oder von Privatpersonen handelt. Auch wenn der Anbieter auf einer Zahlung per Vorkasse besteht, ist Skepsis angebracht. E-Mails, in denen Ihnen Traumjobs mit enormen Verdienstmöglichkeiten bei geringstem Arbeitseinsatz versprochen werden oder Sie für einen vermeintlichen Lotteriegewinn zunächst einmal eine Gebühr zahlen sollen, können Sie ruhigen Gewissens in den Papierkorb verschieben, denn hier drohen Ihnen Ärger und finanzielle Einbußen.

Die Tabelle zeigt die Risiken beim Surfen und die jeweiligen Schutzmaßnahmen, die Gegenstand der folgenden Kapitel sind.

SCHADSOFTWARE	PHISHING UND IDENTITÄTS-DIEBSTAHL	ABHÖREN UND UNERWÜNSCHTE DATENWEITER-GABE	BETRÜGEREIEN BEIM ONLINE-BANKING UND ONLINESHOPPING
Nutzung eines Antivirenprogramms. Sicheres Betriebssystem und sichere Anwendungen durch Aktualisierungen. Aktivierung von Browsersicherheitsfeatures wie Phishing-Filtern. Verwendung zusätzlicher Sicherheitstools (Brower-Plug-ins). Vorsicht beim Download von Software. Vorsicht beim Anklicken von Links.	Vorsicht bei E-Mails mit Fragen zu persönlichen Daten und Zugangsdaten (PIN, Passwörter etc.). Vorsicht bei Chat-Anfragen zu persönlichen Daten und Zugangsdaten. Vorsicht auf Webseiten und bei neuen Browserfenstern, bei denen derartige Daten abgefragt werden. Verwendung ausreichend sicherer Passwörter.	Nutzung von Verschlüsselungslösungen für die Kommunikation (E-Mail, Chat etc.). Nutzung von Werbeblockern und ähnlichen Tools. Nutzung von Widerspruchslösungen (Do-not-Track etc.). Restriktive Cookie-Einstellungen. Verwendung von VPN-Verbindungen. Verwendung von Anonymisierungsdiensten.	Verwendung moderner Onlinebanking-Sicherheitssysteme. Überprüfung der Seriosität von Onlineshops. Nutzung sicherer Onlinezahlungsverfahren. Skepsis bei Billigangeboten unbekannter Anbieter. Vorsicht bei Zahlung per Vorkasse. Nutzung sicherer Anmeldeverfahren und sicherer Passwörter.

ALLGEMEINE SICHERHEITS-MASSNAHMEN

2

Die Sicherheit beim Surfen hängt ganz wesentlich von der Sicherheit der Zugangsgeräte ab. Sind auf den verwendeten Rechnern Schwachstellen vorhanden, können Schadprogramme eindringen und Daten ausspionieren. Der Rechner kann auch ferngesteuert und zu kriminellen Zwecken missbraucht werden. Nicht alle Rechnerplattformen sind gleichermaßen gefährdet. Bei Desktop-PCs und Notebooks müssen sich vor allem Windows-Anwender Sorgen machen, im Bereich von Smartphones und Tablets leben vorwiegend Android-Nutzer gefährlich.

Als Heimanwender sollten Sie auch den Router absichern, über den Sie Ihre Geräte mit dem Internet verbinden. Die wichtigste Schutzmaßnahme bei Routern ist die Zugangssicherung des WLAN, die eine unerwünschte Nutzung des Anschlusses durch Dritte verhindert. Neben der Sicherheit aller beteiligten Geräte gehört auch die Nutzung sicherer Passwörter zu den elementaren Schutzmaßnahmen.

2.1 Schutz für Windows-Rechner

Bei Desktop-PCs und Notebooks sind vor allem Windows-Rechner durch Schadsoftware bedroht, während Apple-Computer und Linux-Rechner weitgehend verschont bleiben. Dies ist primär dadurch bedingt, dass die Masse der Windows-Nutzer ein deutlich lukrativeres Angriffsziel darstellt als die Minderheit der Mac-OS- und Linux-Anwender. Die Entwickler der Schadprogramme haben auch keine unendlichen Ressourcen und versuchen, das Optimum herauszuholen, indem sie sich auf das wichtigste Angriffsziel konzentrieren.

Antivirenprogramme unverzichtbar

Als Windows-Nutzer sollten Sie auf keinen Fall auf ein aktuelles Antivirenprogramm verzichten. Ohne eine solche Schutzsoftware setzen Sie sich völlig unnötig einer großen Gefahr aus. Wenn Sie Onlinebanking mit Ihrem Rechner betreiben, ist der Einsatz eines aktuellen Schutzprogramms absolut unverzichtbar. Kommt es zu einem Schadensfall durch einen Banking-Trojaner, erstatten die Banken den Schaden nur, wenn der Kunde nachweisen kann, dass er sich nicht grob fahrlässig verhalten und eine aktuelle Schutzsoftware eingesetzt hat.

WINDOWS DEFENDER IST NUR EIN PROVISORIUM

Microsoft hat in den Versionen ab Windows 8 ein Antivirenprogramm eingebaut, sodass ein neuer Rechner gleich vom Start an geschützt ist. Allerdings hat sich in unabhängigen Tests immer wieder gezeigt, dass dieses Schutzprogramm namens Windows Defender unterdurchschnittlich abschneidet. Auch Microsoft selbst sieht dieses Programm daher nicht als Dauerlösung, sondern empfiehlt es als Zwischenlösung, damit Sie sich nach der Neuinstallation des PCs in Ruhe nach einem höherwertigen Antivirenprogramm umsehen können und auch dann einen gewissen Grundschutz haben, wenn Sie vergessen, das Abo für Ihr vorhandenes Antivirenprogramm zu verlängern, und nicht mehr mit aktuellen Virenmustern beliefert werden.

Für ein brauchbares Antivirenprogramm müssen Sie nicht unbedingt Geld ausgeben, es gibt auch einige Gratisangebote, die gut funktionieren. Allerdings müssen Sie bei diesen Produkten mit einigen Einschränkungen leben und etwa Werbeeinblendungen akzeptieren. Auch werden Sie regelmäßig auf die Vorzüge der kostenpflichtigen Versionen hingewiesen, die einige zusätzliche Funktionen enthalten. Wenn Ihnen derartige Einschränkungen und Beeinträchtigungen nichts ausmachen, können Sie Ihren PC beispielsweise sehr gut mit den Gratisversionen Avira Free Antivirus oder avast! Free Antivirus schützen.

DER PREIS IST KEIN QUALITÄTSINDIKATOR

Generell gibt der Preis eines Antivirenprogramms keinen zuverlässigen Hinweis auf die Qualität der Software. Ein günstiges Produkt kann durchaus einen besseren Schutz bieten als ein teureres Programm. Allerdings sind die Preisunterschiede ohnehin nicht sehr groß. Die meisten Antivirenprogramme kosten im Jahresabonnement zwischen 20 und 40 Euro.

In totaler Sicherheit dürfen Sie sich bei Verwendung eines Antivirenprogramms nicht wiegen, einen absoluten Schutz vor Schadprogrammen kann keine Anwendung bieten. Erkennungsquoten von 90 Prozent sind schon recht gut, teilweise werden sogar 95 bis 98 Prozent erreicht, was allerdings nur wenige Programme schaffen. Am anderen Ende des Spektrums stehen dagegen Erkennungsraten von 50 bis 65 Prozent, was bedeutet, dass diese Antivirenprogramme jede zwei-

te bzw. jede dritte Malware unbemerkt passieren lassen. Das ist zwar immer noch besser als nichts, beruhigend ist es jedoch nicht.

Antivirenprogramme gibt es auch zum Nulltarif wie etwa von Avira.

Bei aktuellen Tests (Stand: Anfang 2015) zeichneten sich folgende Programme durch die höchsten Erkennungsquoten aus:

- Kaspersky Anti-Virus 2015
- Trend Micro Antivirus + Security
- F-Secure Antivirus
- Norton Security (Symantec)
- avast! Antivirus (Free- und Pro-Version)

Bei diesen Angaben sollten Sie allerdings daran denken, dass es sich um eine Momentaufnahme handelt. Schon oft ist es passiert, dass Hersteller von Antivirenprogrammen, die in aktuellen Tests eher schlecht abschnitten, Konsequenzen zogen und umgehend ein deutlich verbessertes Produkt anbieten konnten, während sich umgekehrt Testsieger auf den Lorbeeren ausruhten und anschließend nicht mehr so gut abschnitten.

IMMER NUR EIN ANTIVIRENPROGRAMM VERWENDEN

Auf einem Rechner sollten Sie immer nur ein Antivirenprogramm im Einsatz haben. Es kann sonst zu unerwünschten Nebenwirkungen und Problemen kommen, wenn beispielsweise die Virenmuster aus den Updates des einen Programms in der anderen Software als potenziell gefährliche Dateien eingestuft werden. Außerdem sollten Sie das Antivirenprogramm so einstellen, dass regelmäßig ein Komplettscan des Rechners durchgeführt wird. Damit können auch solche Schädlinge erkannt werden, die zunächst unerkannt auf den PC gelangt sind und hier beispielsweise in Zip-Dateien eine potenzielle Gefahr darstellen.

Je länger ein Schadprogramm in Umlauf ist, desto mehr Antivirenprogramme erkennen es. Wenn in Ihrem Posteingang eine verdächtige E-Mail mit Dateianhang angekommen ist, Sie aber nicht ausschließen können, dass es sich doch um eine harmlose Datei handelt, kann es durchaus empfehlenswert sein, einige Tage zu warten und die Datei anschließend mit dem Antivirenprogramm noch einmal zu scannen.

ONLINEVIRENSCANNER ALS ZUSÄTZLICHE OPTION

Ebenfalls hilfreich können in Verdachtsfällen Onlinevirenscanner sein. Bei den meisten Angeboten können Sie verdächtige Dateien auf einen Internetserver übertragen, auf dem sie dann untersucht werden. Es gibt aber auch (kostenpflichtige) Dienste, die ganze Ordner oder Laufwerke untersuchen. Mit diesen Onlineangeboten können Sie die Einschränkung, dass auf einem Rechner immer nur eine Antivirensoftware genutzt werden soll, umgehen. Sie sollten daher stets den Onlinedienst eines anderen Herstellers verwenden und nicht auf denselben Anbieter zurückgreifen, dessen Software Sie ohnehin schon auf Ihrem Rechner nutzen. Diese Systeme verwenden dieselben Virenmuster und werden daher auch zu den gleichen Ergebnissen kommen. Einen vollwertigen Ersatz für eine installierte Antivirensoftware bilden die Onlinevirenscanner allerdings nicht, da hier der permanente Schutz beim Zugriff auf die Dateien nicht vorhanden ist. Bekannte Onlinevirenscanner sind Virus Total (*www.virustotal.com*) oder Housecall von Trend Micro (*housecall.trendmicro.com/de*).

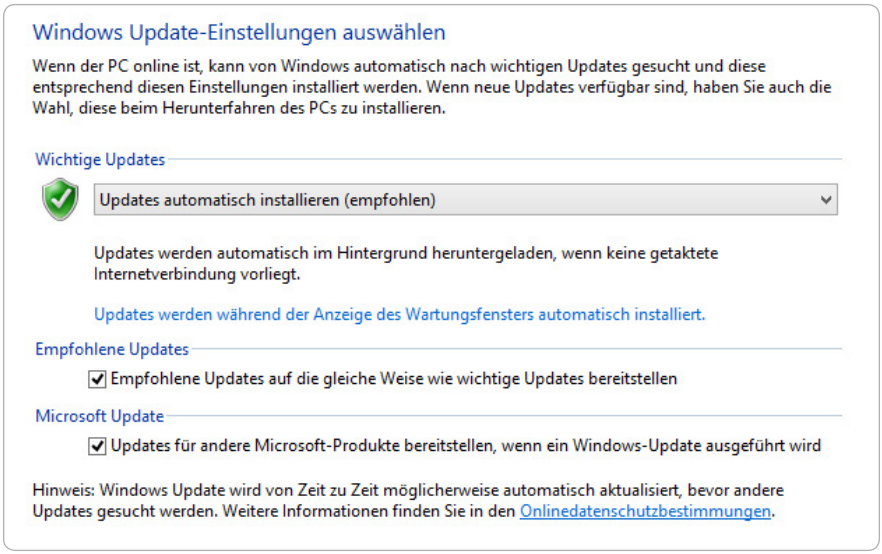
Mit einem Onlinevirenscanner können Sie eine zweite Meinung einholen.

Betriebssystem und Anwendungen aktualisieren

Ebenso wichtig wie die Nutzung eines Schutzprogramms ist es, eventuell vorhandene Schwachstellen zu eliminieren, die sich Schadprogramme zunutze machen, um auf den Rechner zu gelangen und Unheil anzurichten.

Schwachstellen lauern nahezu überall. Sowohl im unverzichtbaren Betriebssystem als auch in Anwendungen kommen sie vor. Ist solch eine Sicherheitslücke erst einmal bekannt und veröffentlicht, benötigen Trojaner-Programmierer nur wenig Zeit, um ihre Schadsoftware so anzupassen, dass sie auf diesem Weg Rechner infiltrieren kann. Erst wenn die Entwickler des Betriebssystems oder der betroffenen Anwendung die Schwachstelle durch Patches und Updates beseitigt haben, droht keine Gefahr mehr.

Um sich zu schützen, müssen Sie daher sicherheitsrelevante Updates bzw. Patches möglichst unverzüglich nach Erscheinen installieren. Für Windows, aber auch für viele andere weitverbreitete Anwendungen, etwa die für die Internetnutzung unverzichtbaren Browser sowie weitverbreitete Browsererweiterungen, gibt es bereits seit einiger Zeit automatische Updates. Damit müssen Sie sich kaum noch um etwas kümmern, da Updates automatisch heruntergeladen und installiert werden. Viele andere Softwarehersteller haben nach einigem Zögern ebenfalls auf diese Art der Aktualisierung umgestellt, allerdings gibt es nach wie vor auch noch Anwendungen, bei denen Sie manuell tätig werden müssen.

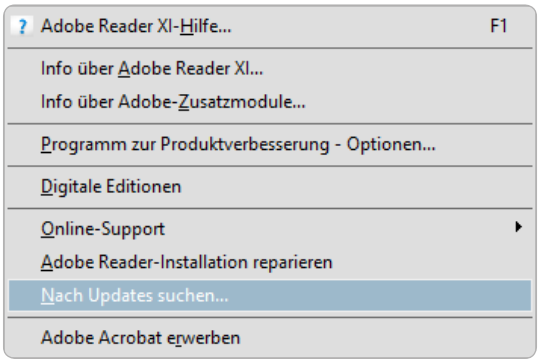


Das Windows-Update sollte auf Ihrem PC automatisch durchgeführt werden.

AUTO-UPDATE-EINSTELLUNG ÜBERPRÜFEN

Unter Windows sollte das Auto-Update aktiviert sein. Sie können dies kontrollieren, indem Sie in der *Systemsteuerung* unter dem Punkt *Windows Update* nachsehen, ob die Option *Updates automatisch installieren* aktiviert ist. Hier können Sie auch festlegen, dass Updates für andere Microsoft-Programme (wie etwa Microsoft Office) bereitgestellt werden. Außerdem empfiehlt es sich, regelmäßig nachzuschauen, ob die Updates auch erfolgreich durchgeführt wurden. Dazu klicken Sie auf den Eintrag *Updateverlauf anzeigen*.

Immerhin haben die allermeisten Programme eine Funktion, mit der Sie überprüfen können, ob die genutzte Programmversion noch aktuell oder bereits eine neuere Version verfügbar ist. Diese Abfrage finden Sie im *Hilfe*-Menü. Wird eine neue Version angeboten, sollten Sie umsteigen, da bei älteren Versionen Sicherheitslücken nicht mehr geschlossen werden, sodass das Risiko deutlich höher ist als bei aktuellen Versionen.



Über das *Hilfe*-Menü können Sie bei vielen Programmen nach aktuellen Updates suchen.

Als Sicherheitsrisiken gelten vor allem Programme und Tools, die direkt beim Surfen zum Einsatz kommen. Neben dem Browser gehören dazu auch Browsererweiterungen und Plug-ins, etwa zum Anzeigen oder zur Wiedergabe von Multimedia-Inhalten oder anderen Dateiformaten. Lange Zeit standen bei Angreifern PDF-Programme im Fokus, bei denen immer wieder Sicherheitslücken gefunden werden. Schon das Öffnen eines scheinbar harmlosen und unverdächtigen PDF-Dokuments kann zu einer Infektion des Rechners führen.

VORSICHT BEI FLASH

Als Anfang 2015 kurz hintereinander mehrere gravierende Schwachstellen im Flash-Player von Adobe entdeckt wurden, gab es eine regelrechte Flash-Angriffswelle. Das Flash-Format ist im Web sehr verbreitet und die Flash-Software auf nahezu jedem Rechner vorhanden. Besonders brisant an diesen Vorfällen war, dass Adobe längere Zeit brauchte, um nach dem Bekanntwerden der Schwachstellen die notwendigen Updates bereitzustellen. In der Zwischenzeit wurde diese Lücke durch Hacker in großem Umfang ausgenutzt. Sicherheitsbewussten Anwendern blieb nichts anderes übrig, als Flash für diesen Zeitraum zu deaktivieren.

Das Ausnutzen einer bekannten Schwachstelle, für die es vom Softwareanbieter noch keinen Patch gibt, wird als Zero-Day-Exploit bezeichnet. Als Anwender sind Sie derartigen Angriffen weitgehend schutzlos ausgeliefert, es sei denn, Sie deaktivieren die betroffene Software und verzichten auf die Nutzung, bis das Problem behoben ist.

Je mehr Anwendungen Sie auf Ihrem Rechner installiert haben, desto mehr potenzielle Schwachstellen sind vorhanden. Damit steigt auch der Aufwand, den Sie betreiben müssen, um Programme auf Aktualität zu überprüfen und mit Updates zu versorgen. Sie sollten daher vor jeder Neuinstallation einer Software genau überlegen, ob Sie die zusätzliche Anwendung überhaupt benötigen. Es kann hilfreich sein, Programme, die Sie lange Zeit nicht mehr benutzt haben, zu deinstallieren. Damit schalten Sie nicht nur eine potenzielle Gefahrenquelle aus, sondern verfügen auch wieder über mehr Speicherplatz.

2.2 Router und WLAN absichern

Beim Surfen in den heimischen vier Wänden verwenden Sie in aller Regel einen Router und ein Drahtlosnetzwerk (WLAN). Andere Techniken wie etwa das Modem, das an einen einzelnen Rechner angeschlossen wird, spielen dagegen kaum noch eine Rolle. Allein schon die Nutzung eines Routers sorgt für mehr Sicherheit, da in diesem Gerät bereits einige Schutzmechanismen integriert sind.

Normalerweise sind Router bereits so vorkonfiguriert, dass Sie nach Anschluss und Konfiguration sofort loslegen können und sich nicht um irgendwelche Einstellungen kümmern müssen. Allerdings gibt es auch bei Routern Sicherheitslücken. Diese ermöglichen es Angreifern, Ihr WLAN-Passwort auszuspionieren, sodass sie Ihren Internetzugang verwenden können. Das kann für Sie unangenehme Folgen haben, wenn über Ihren Internetzugang urheberrechtlich geschützte Filme oder Musik illegal heruntergeladen werden. Da diese Aktivitäten nur bis zum Anschluss zurückverfolgt werden können, wird der Anschlussinhaber dafür verantwortlich gemacht.

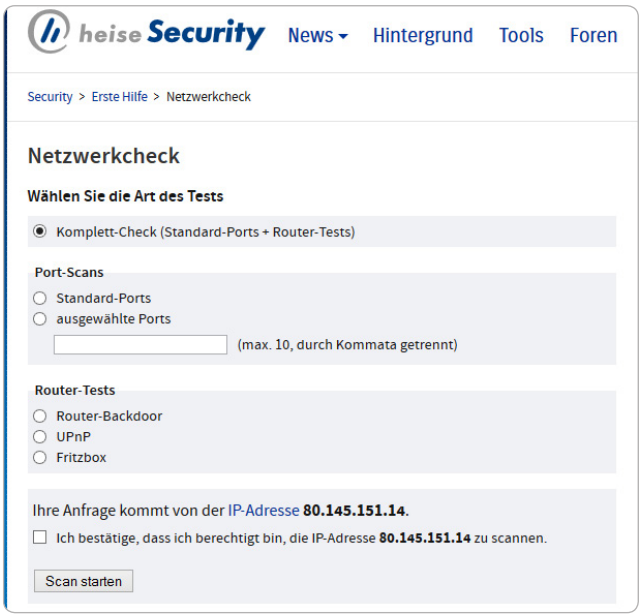
Eine bekannte Schwachstelle, über die sich Angreifer Zugang zu den Routern verschaffen können, ist die UPnP-Option, eine weitere weitverbreitete Schwachstelle betrifft die WPS-Funktion, über die sich die Anbindung von WLAN-Geräten an den Router einfacher und schneller durchführen lässt, da statt eines komplexen Passworts nur eine einfache PIN zur Anmeldung eines neuen Geräts ausreicht oder die Anbindung per Knopfdruck geschieht.

2014 wurde eine andere Sicherheitslücke bekannt, die erhebliche Konsequenzen hatte, da sie über längere Zeit unentdeckt ausgenutzt werden konnte. Betroffen waren allerdings nur Internetanschlüsse, bei denen Nutzer auch per VoIP über das Internet telefonierten und bestimmte Routermodelle von AVM

nutzten. Die Schwachstelle ermöglichte es Angreifern, VoIP-Telefonate zu führen, ohne dass die Anschlussinhaber davon etwas mitbekamen. Es wurden teure Auslandstelefonate geführt und Servicerufnummern auf Kosten der Opfer angerufen. Zwar bot Routerhersteller AVM nach einiger Zeit ein Firmware-Update für die betroffenen Modelle an, jedoch nutzten viele Anwender diese Option zunächst nicht, sodass deren Router nach wie vor anfällig blieben.

ONLINETEST FÜR ROUTER

Ob Ihr Router auch von einer dieser Lücken betroffen ist, können Sie online überprüfen. Unter anderem bietet das Computermagazin c't in Zusammenarbeit mit dem Datenschutzbeauftragten aus Niedersachsen einen Check an. Sie erreichen den Dienst über die Webadresse *http://www.heise.de/security/dienste/portscan/test/go.shtml?scanart=1*. Mit diesem Test können Sie Ihren Router auch auf andere Schwachstellen hin untersuchen lassen.



Ein Onlinesicherheitstest zeigt Ihnen mögliche Schwachstellen Ihres Routers.

WLAN absichern

In jedem Fall sollten Sie Ihr WLAN verschlüsseln, damit nicht unberechtigte Dritte über Ihren Internetzugang surfen. Alle halbwegs modernen WLAN-Router und WLAN-fähigen Endgeräte unterstützen den Verschlüsselungsstandard WPA2, der sicher ist und schnelle Verbindungen erlaubt. Der direkte Vorgänger WPA bietet auch zuverlässigen Schutz, hinkt jedoch bei der Übertragungsgeschwindigkeit mittlerweile hinterher und bremst besonders schnelle Internetanschlüsse (wie VDSL) aus.

WEP BIETET KEINEN SCHUTZ MEHR

Auf die Nutzung des veralteten Standards WEP sollten Sie verzichten, da dieses Verfahren schon vor Jahren geknackt wurde. Haben Sie noch Uraltgeräte mit WEP im Einsatz, sollten Sie unbedingt neue Hardware anschaffen, da eine sichere Verschlüsselung damit nicht möglich ist.

Ältere WLAN-Geräte beherrschen WPA2 noch nicht, sodass viele Router auch einen Mixed-Modus aus WPA/WPA2 bieten, in dem beide Verfahren parallel betrieben werden. Dabei kann lediglich die WPA-Geschwindigkeit von maximal 54 MBit/s genutzt werden. Wenn alle Geräte, mit denen Sie zu Hause ins Internet gehen, WPA2 unterstützen, sollten Sie am Router ausschließlich WPA2 mit CCMP-Protokoll und AES-Verschlüsselung wählen. Eventuell lassen sich Geräte, die zunächst nur WPA unterstützen, mit einem Firmware-Upgrade auf WPA2 aktualisieren, sodass Sie anschließend vom Mixed-Modus in den schnelleren WPA2-Modus wechseln können, ohne diese Geräte auszusperren.

WLAN-Passwort

Die meisten Router werden mit eingeschalteter Verschlüsselung ausgeliefert. Auf den Zugangsgeräten müssen Sie das voreingestellte WLAN-Passwort eingeben, um eine Verbindung aufbauen zu können. Manche Router bieten auch einfachere Lösungen zur schnellen Hardwareanbindung, die aber mit zusätzlichen Risiken verbunden sind, wie das bei der erwähnten WPS-Sicherheitslücke der Fall ist.

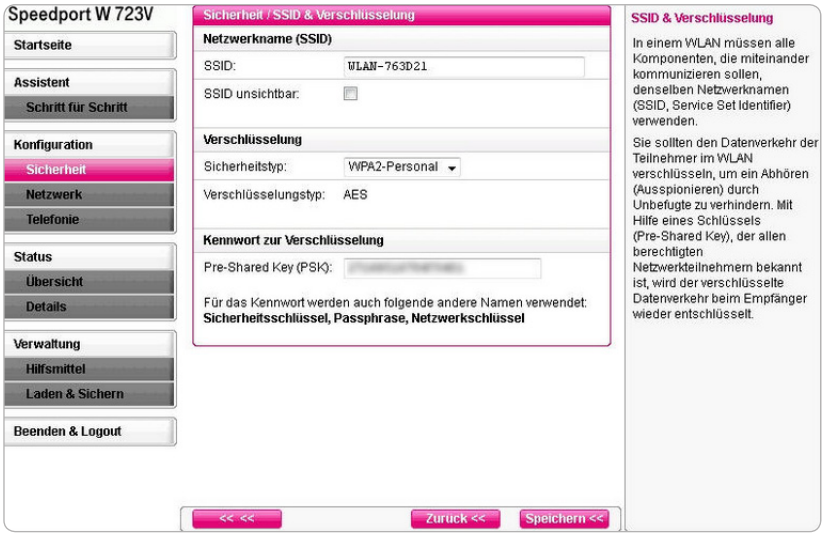
Bei einigen Geräten kann das Originalpasswort mit etwas Aufwand rekonstruiert werden, weil die Hersteller es aus anderen Daten abgeleitet haben. Diese

Router sind dadurch für Angriffe anfällig und bieten mit dem Originalpasswort keine ausreichende Sicherheit. Ebenso gibt es viele Router, bei denen das Passwort auf dem Gerät angebracht ist und abgelesen werden kann. Personen, die Zugang zu Ihrer Wohnung hatten und das Passwort notieren oder fotografieren konnten, können Ihren Internetzugang nutzen, ohne dass Sie es merken.

WLAN-PASSWORT ÄNDERN

Ändern Sie nach der Inbetriebnahme des Routers das WLAN-Passwort schnellstmöglich. Die Änderung des Passworts gehört auch nach Ansicht deutscher Gerichte zu den Minimalanforderungen, die der Inhaber eines Internetanschlusses erfüllen muss, um sich bei möglichen juristischen Auseinandersetzungen wegen Missbrauchs seines Anschlusses nicht grobe Fahrlässigkeit vorwerfen lassen zu müssen.

Über das Konfigurationsmenü lässt sich das WLAN-Passwort des Routers sehr einfach ändern. Sie sollten ein vergleichsweise langes Passwort verwenden, da mit zunehmender Zeichenzahl die Sicherheit steigt. Ab einer Länge von



Das vom Hersteller voreingestellte WLAN-Passwort müssen Sie unbedingt ändern.

16 Zeichen sind Sie auf der sicheren Seite, selbst wenn Sie einfache Zeichenfolgen wählen, 20 Zeichen sind in jedem Fall ausreichend. Da das Passwort auf den Zugangsgeräten gespeichert und nicht für jedes Anmelden benötigt wird, ist der Nutzungskomfort nicht beeinträchtigt. Es spricht auch kaum etwas dagegen, wenn Sie sich dieses Passwort notieren, sofern Sie die Aufzeichnung halbwegs sicher aufbewahren. Da Sie dieses Passwort nur selten benötigen, werden Sie es sich kaum einprägen können.

Weitere Schutzmaßnahmen zur WLAN-Absicherung sind unnötig. Zwar finden sich immer wieder Tipps beispielsweise zum Abschalten der Übertragung des Funknetznamens (SSID) oder zur Filterung der MAC-Adressen, allerdings ist der Schutzeffekt dieser Maßnahmen eher begrenzt, während zugleich der Nutzungskomfort beeinträchtigt wird. Der Gebrauch einer sicheren Verschlüsselung (möglichst WPA2) und eines hinreichend langen Passworts reicht vollkommen aus, um das eigene WLAN anständig abzusichern.

2.3 Schutz für Smartphones und Tablets

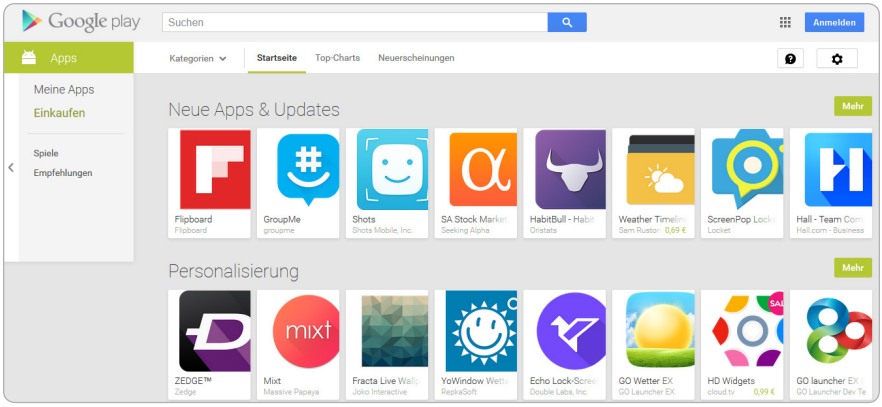
In der Welt der Smartphones und Tablets verhält es sich ähnlich wie bei Notebooks und Desktops, denn auch hier ist eine Plattform besonders riskant – Android. Während iPhones und iPads von Apple, BlackBerry-Geräte und auch Smartphones mit Windows Phone als recht sicher gelten, hat es bei Android schon einige Attacken durch Schadsoftware gegeben. Auch Anwender, die noch alte Smartphones mit Symbian verwenden, sind stark gefährdet, allerdings spielt dieses Betriebssystem auf dem Markt so gut wie keine Rolle mehr.

Die besondere Anfälligkeit von Android-Systemen gegenüber Schadsoftware liegt daran, dass es möglich ist, Software aus unterschiedlichen Quellen zu installieren. Bei Windows Phone und iOS gibt es eine strikte Beschränkung auf die App-Stores von Microsoft und Apple, in denen Apps vor der Veröffentlichung intensiv geprüft werden und Entwickler sich registrieren lassen müssen. Dadurch reduziert sich das Risiko, dass sich eine App als Trojaner entpuppt, ganz erheblich.

Auf den anderen Plattformen sind Angriffe durch Schläfer-Apps ebenfalls denkbar, sodass Sie auch hier Vorsicht walten lassen sollten. Ebenso sollten Sie bei iPad und iPhone auf das Jailbreaking verzichten, durch das das Gerät entsperrt wird und anschließend Apps aus anderen Quellen installiert werden können. Das Risiko wird dadurch unnötig erhöht.

AUCH APPS AUS DEN APP-STORES KÖNNEN PROBLEMATISCH SEIN

Betrüger haben sich einige Tricks einfallen lassen, um die Schutzmechanismen der offiziellen App-Stores auszuhebeln. So wurde kürzlich ein Trojaner in Google Play, dem offiziellen App-Store von Google, enttarnt, der lange Zeit unentdeckt geblieben war, weil die Schadfunktion erst nach einigen Monaten aktiv wurde und die Software bei den Überprüfungen zunächst unauffällig blieb. Bis die unerwünschten Zusatzfunktionen in den Spiele-Apps auffielen, waren bereits Millionen Android-Geräte infiziert, die unerwünschte Werbung einblendeten und Nutzer auf Seiten leiteten, auf denen weitere Schadsoftware verteilt wurde.



Selbst in die offiziellen App-Stores können sich Schadprogramme einschleichen.

Dennoch ist die Gefahrenlage bei den anderen Mobilplattformen sehr überschaubar. Zwar hat es mit WireLurker einen Trojaner gegeben, der von infizierten Mac-Rechnern und Windows-PCs aus auf iPhones und iPads übertragen werden konnte, doch blieben derartige Angriffe bislang die absolute Ausnahme. Für Windows Phone und iOS benötigen Sie daher noch keine Antivirensoftware, bei Android hingegen sollte eine solche Schutzsoftware zur Grundausstattung gehören. Dies gilt vor allem dann, wenn Sie über das Mobilgerät Onlinebanking betreiben oder mTANs empfangen. Für Android-Smartphones gibt es Trojaner, mit denen Bankdaten abgefangen werden können.

Schutzsoftware für Android

Die Rechenleistung moderner Smartphones ist meist so hoch, dass die zusätzliche Belastung durch die Antivirensoftware, die ja permanent im Hintergrund läuft, kaum spürbar ist. Auch auf die Akkulaufzeit haben diese Programme kaum Auswirkungen. Befürchtungen, dass die Leistung und Nutzbarkeit der Geräte durch die Antivirensoftware stark beeinträchtigt sein würden, treffen nur in Ausnahmefällen zu.

Zu den besten Antivirenprogrammen für Android gehören laut Vergleichstest der unabhängigen Testorganisation AV-Test Ende 2014 folgende Produkte:

- Sophos Mobile Security 4.0
- Trend Micro Mobile Security 6.0
- Kaspersky Internet Security 11.5
- GData Internet Security 25.6
- Antiv AVL

Android hat ein weiteres sicherheitsrelevantes Manko gegenüber anderen Mobilplattformen, weil es bei Android-Hardware keine einheitliche Update-Politik gibt. Dies wird dann problematisch, wenn Sie ein Gerät mit einer älteren Android-Version verwenden, für das kein Update angeboten wird und das von einer sicherheitsrelevanten Lücke betroffen ist.

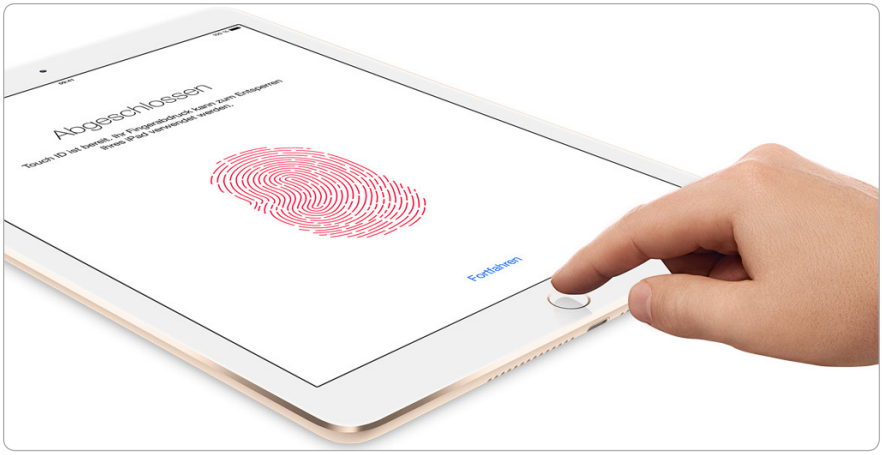
VORSICHT BEI ANDROID-BROWSERN

Ein aktuelles Beispiel ist die Browser-App älterer Android-Versionen bis einschließlich 4.3. Dieser Browser hat eine Schwachstelle, durch die Schadsoftware eingeschleust werden kann. Obwohl das Leck schon seit Längerem bekannt ist, wird es auch künftig kein Sicherheitsupdate geben. Wenn der Hardwarehersteller für das Gerät kein Update auf eine aktuellere Android-Version anbietet, bleibt diese Lücke offen. Als Abhilfe für diesen konkreten Fall empfiehlt Google allen Anwendern, auf einen anderen Browser als den mitgelieferten umzusteigen. Dieser muss allerdings eine eigene Rendering-Engine mitbringen, wie es bei Firefox oder Chrome der Fall ist.

Sicherheit für unterwegs

Da man Tablets und vor allem Smartphones fast immer dabeihat, steigt das Risiko, dass sie abhandenkommen, weil man sie einfach liegen lässt oder verliert oder weil sie gestohlen werden. Bei Verlust besteht die Gefahr, dass vertrauliche Daten in falsche Hände geraten. Besonders brisant kann es werden, wenn der Dieb oder unehrliche Finder sogar an Passwörter gelangt und damit auf Cloudspeicher oder E-Mail-Postfächer zugreifen kann.

Zum Schutz vor Missbrauch durch Dritte sollten Sie daher Ihr Smartphone oder Tablet in jedem Fall durch eine Gerätesperre sichern. Entsprechende Funktionen sind bei allen Geräteplattformen bereits enthalten. Meistens wird zum Entsperren ein Passwort oder eine PIN benötigt, optional kann auch ein Muster auf dem Touchscreen „gewischt" werden. Einige Modelle der teuren Oberklasse bieten sogar einen Fingerabdrucksensor. Dieses Verfahren bietet eine recht hohe Sicherheit und ist sehr bequem. Mit einigem Aufwand lässt sich aber auch ein Fingerabdrucksensor überlisten.



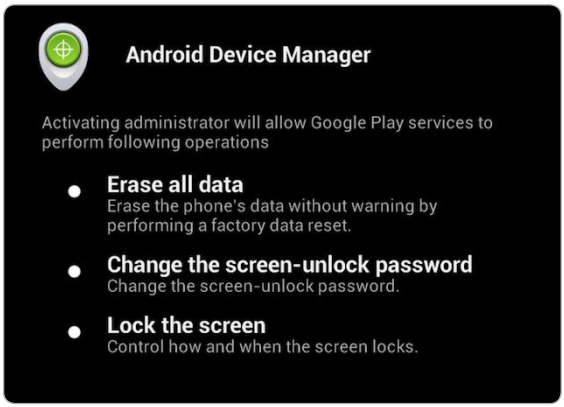
Bei iPhone, iPad und einigen Android-Modellen gibt es Fingerabdrucksensoren. (Foto: Apple)

Die Gerätesperre sorgt etwa beim iPhone auch dafür, dass die Daten verschlüsselt werden, sodass sie nicht auf anderen Wegen ausgelesen werden können. Ähnlich funktionieren viele Android-Modelle. Für Android gibt es auch zahlreiche zusätzliche Verschlüsselungs-Apps, sodass Sie ganz auf Nummer sicher gehen können.

SCHUTZ DURCH ORTUNG UND FERNLÖSCHUNG

Nutzen Sie auch die Optionen zur Ortung und Fernlöschung, die von den Geräteherstellern angeboten werden. Haben Sie Ihr Mobilgerät registriert, können Sie sich über einen Webdienst den aktuellen Standort Ihres Geräts anzeigen lassen, sofern es eingeschaltet ist. Je nach Funktionsumfang ist es dabei sogar möglich, einen Hinweis auf dem Display einzublenden. Besteht das Risiko, dass ein Dieb oder ein unehrlicher Finder versuchen könnte, an die Daten zu gelangen, können Sie alle Inhalte aus der Ferne löschen.

Bei Apple sind diese Ortungs- und Fernlöschungsoptionen in den Clouddienst iCloud integriert, der allen Nutzern kostenfrei zur Verfügung steht. Microsoft bietet einen ähnlichen Service auf seiner Website *windowsphone.com* an, wo Windows-Smartphones auch kostenlos registriert werden. Bei Android haben Sie mehrere Möglichkeiten. Die meisten Gerätehersteller haben hauseigene Lösungen, es gibt aber auch von Google den Android Device Manager und Apps mit Ortungs- und Fernlöschfunktionen. Bekannte IT-Sicherheitsfirmen haben Paketlösungen im Angebot, die Virenschutz, Verschlüsselung, Ortung und Fernlöschung in einer App kombinieren. Diese Sicherheitspakete gibt es auch für iOS und Windows Phone.



Mit dem Android Device Manager können Sie Daten aus der Ferne löschen.

Schnüffelnde Apps

Auf Smartphones und Tablets zeigen einige Apps unerwünschte Nebenwirkungen, indem sie Daten sammeln und ungefragt weiterleiten. Besonders begehrt sind Informationen aus Adressbüchern und Kontaktlisten sowie Standortdaten, aus denen sich Bewegungsprofile erstellen lassen. Vor allem Gratis-Apps fallen in dieser Hinsicht negativ auf, da ihre Anbieter die Informationen verkaufen, um ihre Apps und sich selbst zu finanzieren.

Die Betreiber der App-Stores haben bereits reagiert und blockieren besonders dreiste Ausspähversuche, indem sie den Entwicklern strikte Vorgaben machen. Aber auch als Anwender haben Sie jetzt einige Möglichkeiten, sich darüber zu informieren, welche Berechtigungen Apps sich haben einräumen lassen. Bei neueren iOS-Versionen können Sie genau festlegen, welche Zugriffe einer App erlaubt sein sollen und welche nicht. Für Android gibt es entsprechende Tools wie Clueful von Bitdefender oder AppGuard von SRT, mit denen Sie sich über Berechtigungen informieren und Einstellungen ändern können.

Unter iOS können Sie detailliert festlegen, welche Berechtigungen Apps bekommen sollen.

2.4 Sichere Passwörter

Für eine sichere Internetnutzung spielen Passwörter bis heute (und wohl auch noch in absehbarer Zukunft) eine große Rolle. Bei nahezu allen personalisierten Webangeboten und Onlinediensten wird zur Anmeldung ein Passwort verlangt. Ob Sie sich bei Ihrem E-Mail-Postfach anmelden, beim sozialen Netzwerk eine Nachricht posten, im Onlineshop einkaufen, per Onlinebanking eine Rechnung überweisen, auf Ihren Cloudspeicher zugreifen oder in einem Diskussionsforum einen Beitrag schreiben möchten, überall müssen Sie sich mit einer Kombination aus Benutzername und einem geheimen Passwort anmelden. Auch die PIN (*persönliche Identifikationsnummer*) beim Onlinebanking ist letztlich nur ein numerisches Passwort.

Da Benutzernamen meist öffentlich sind oder häufig aus der E-Mail-Adresse oder dem Realnamen bestehen, sind Passwörter der einzige Schutz vor einem Missbrauch. Die Grundanforderung an jedes Passwort besteht darin, dass es nicht einfach zu erraten oder durch simples Ausprobieren herauszubekommen ist.

Sicherheitsexperten empfehlen, ausschließlich Passwörter zu verwenden, die einen starken Schutz gegen Angriffe bieten. Zu einem sicheren Passwort gehören folgende Merkmale:

- Das Passwort muss ausreichend lang sein. Je nach Zusammensetzung und Verwendungszweck werden 10 bis 20 Zeichen empfohlen. Weniger als 8 Zeichen sollte ein Passwort auf keinen Fall haben.
- Das Passwort sollte auf keinen Fall aus einem »realen« Begriff oder Namen bestehen, da Begriffe über Wörterbuchattacken zu leicht zu enttarnen sind. Auch Geburtsdaten als Ziffernfolge sind zu einfach.
- Das Passwort sollte aus einer Kombination von Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen bestehen. Erst dann ergeben sich so viele Kombinationsmöglichkeiten, dass auch leistungsfähige Hardware zu lange brauchen würde, alle durchzuprobieren.
- Einfache Tastaturmuster wie qwertzuiop oder 1234qwer sind nicht ausreichend, Gleiches gilt für simple Ziffernfolgen wie 00000 oder 11112222.
- Das einfache Voranstellen oder Anhängen eines Sonderzeichens oder einer kurzen Ziffernfolge an einen üblichen Begriff wie passwort01 ist nicht ausreichend.
- Ein und dasselbe Passwort sollte niemals für mehrere Dienste verwendet werden.
- Passwörter sollten niemals zu lange verwendet werden. Zumindest bei besonders schützenswerten Diensten sollten Sie spätestens nach einem halben Jahr das Passwort ändern.
- Ist ein Dienstanbieter, bei dem Sie ein Konto haben, zum Opfer eines Hackerangriffs geworden, sollten Sie dieses Passwort unverzüglich ändern. Haben Sie entgegen der Empfehlung dieses Passwort auch bei anderen Diensten genutzt, sollten Sie dort die Passwörter ebenfalls unverzüglich ändern.

Komplexität vs. Merkbarkeit

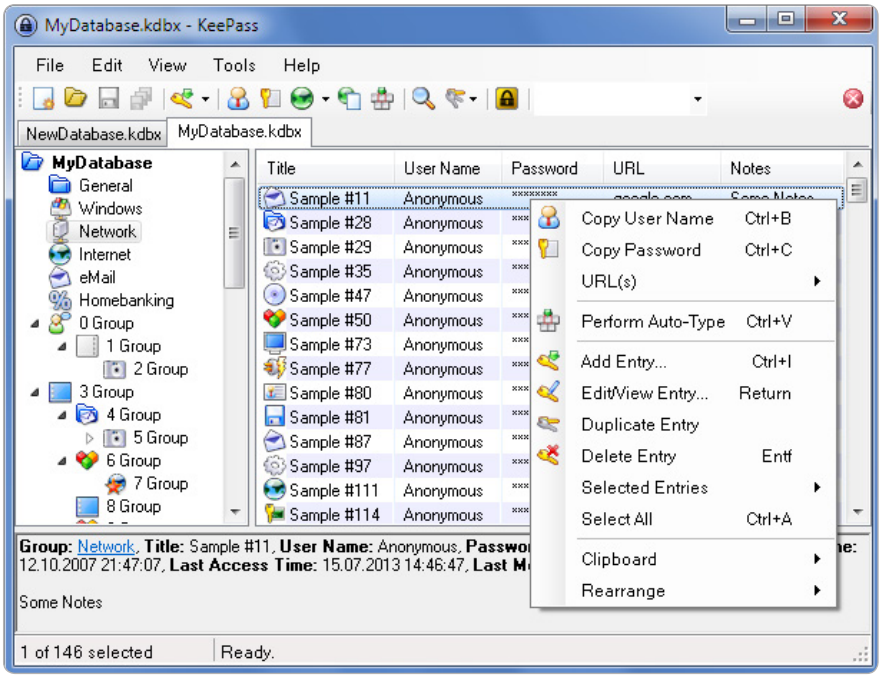
Ein Passwort, das all diesen Vorgaben entspricht, wäre *h6M&Rt9?kA*, allerdings dürfte es auch Menschen mit wirklich gutem Gedächtnis schwerfallen, es sich zu merken. Außerdem benötigen Sie ja nicht nur ein Passwort, sondern je nach Intensität der Internetnutzung ein gutes Dutzend oder noch mehr. Einige davon verwenden Sie mehr oder weniger regelmäßig oder zumindest häufig, wie etwa das Passwort für Facebook, das E-Mail-Konto und ähnliche Dienste, andere dagegen eher selten, wie etwa ein Passwort für einen Onlineshop, in dem Sie vielleicht nur ein oder zwei Mal im Jahr etwas bestellen. Je seltener Sie ein Passwort verwenden, desto geringer dürfte die Chance sein, dass Sie es sich, wenn es wirklich komplex ist, auch tatsächlich merken können.

NICHT OPTIMAL, ABER AKZEPTABEL: PASSWÖRTER NOTIEREN

Im Zweifelsfall kann es angeraten sein, dass Sie sich Passwörter auf Papier notieren, sofern Sie diese Aufzeichnung anschließend gut gesichert aufheben. Auf keinen Fall sollten Sie einen Zettel mit Passwörtern zusammen mit dem Notebook herumtragen oder die Passwortliste offen in der Nähe Ihres Rechners liegen lassen. Sichere und komplexe Passwörter, die Sie sich aufschreiben, sind jedoch besser als zu einfache oder mehrfach genutzte Passwörter, solange Sie die Liste an einem sicheren Ort aufbewahren.

Es gibt auch die Möglichkeit, Passwörter in Passwortsafes auf dem Rechner selbst zu speichern. Die Passwörter werden verschlüsselt gespeichert und können mit einem Masterpasswort sichtbar gemacht oder direkt übernommen werden. Ein bekannter Passwortsafe aus dem Open-Source-Bereich ist KeePass. Die meisten Browser, wie der Internet Explorer, Firefox und Chrome, bieten ähnliche Funktionen und merken sich Benutzernamen und Passwörter.

Allerdings haben Passwortspeicherlösungen auch Risiken und Nachteile. Wird das Masterpasswort geknackt, stehen alle gesicherten Konten offen. Nutzen Sie mehrere Rechner, benötigen Sie auf allen Rechnern eine solche Lösung, und wollen oder müssen Sie einmal von einem fremden Rechner aus ins Internet, steht Ihnen ein lokal installierter Passwortsafe nicht zur Verfügung. Speichern Sie die Passwörter über eine Safelösung in der Cloud, sodass Sie von überall aus Zugriff darauf haben, müssen Sie dem Anbieter vertrauen, dass Ihre Daten dort wirklich sicher sind.



KeePass ist ein zuverlässiger Passwortsafe, der kostenfrei nutzbar ist.

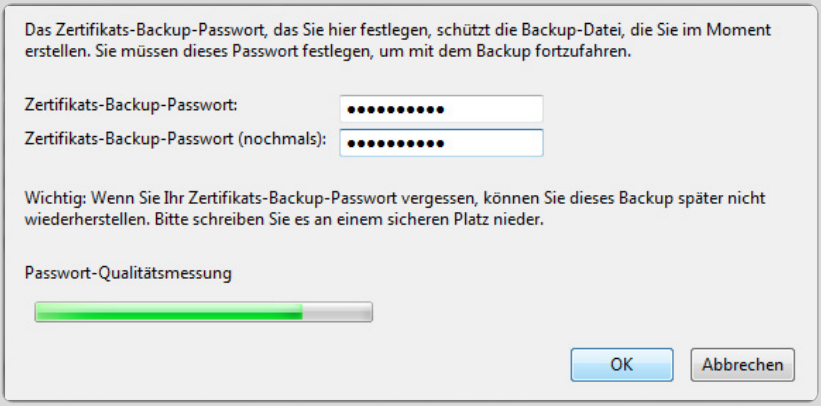
Praxislösung

Privatpersonen müssen nicht für alle Bereiche unbedingt die allerhöchsten Sicherheitsanforderungen für Passwörter in vollem Umfang beachten. Wenn Sie sich beispielsweise für ein Diskussionsforum registrieren, reicht auch ein nicht ganz vorschriftsmäßiges Passwort aus, sofern es sich nicht um eine zu banale Variante handelt. Es wird wohl kaum jemand mit erheblichem Aufwand Ihr Passwort für ein Forum knacken, um dann unter Ihrem Namen dort aktiv zu werden. In derartigen Fällen, in denen der Schutz nicht ganz so wichtig ist, reicht ein halbwegs sicheres und gut merkbares Passwort aus.

Bei wichtigen Diensten sollten Sie auf Nummer sicher gehen und Passwörter verwenden, die hohen Ansprüchen genügen. E-Mail-Postfächer sollten unbedingt bestmöglich abgesichert werden, denn über das E-Mail-Konto können oft ja auch die Passwörter für andere Dienste geändert werden. Außerdem

BEACHTEN SIE DEN EINGEBAUTEN QUALITÄTSCHECK

Auf vielen Registrierungsseiten haben Dienstanbieter eine Prüfung der Passwortqualität eingebaut, und auch bei vielen Anwendungen wird die Qualität der Passwörter beurteilt. Bei der Eingabe des Passworts wird Ihnen angezeigt, ob Ihr Passwort ausreichende Sicherheit bietet oder nicht. Auch bei nicht ganz so wichtigen Diensten sollten Sie die Hinweise der Qualitätsprüfung beachten und das Passwort nicht zu kurz und zu einfach wählen.



Viele Sicherheitstools und Anwendungen prüfen die Qualität Ihres Passworts.

enthalten Ihre E-Mails selbst Informationen, die von Hackern gezielt für weitere Attacken missbraucht werden könnten. Auch Konten bei Onlineshops und Zahlungsdiensten sollten Sie unbedingt mit bombensicheren Passwörtern schützen. Es gibt einige Tricks, mit denen Sie kaum knackbare Passwörter kreieren können, die Sie sich einigermaßen gut merken können.

Zwei-Komponenten-Passwort

Eine simple, aber durchaus brauchbare Option besteht darin, dass Sie die Passwörter in zwei Komponenten aufteilen. Ein Teil ist für alle Passwörter gleich, der zweite Teil dagegen speziell auf die jeweiligen Konten abgestimmt. Der überall verwendete Teil sollte aus einer möglichst zufälligen Folge von Groß- und Kleinbuchstaben sowie Ziffern und Sonderzeichen bestehen.

Für diesen Passwortkern reichen schon sechs oder sieben Zeichen aus. Ein Beispiel wäre etwa *zN7m&!T*. Diese Kernkomponente kann man sich relativ gut merken. Zur Not bilden Sie einen Merksatz oder Ähnliches, nehmen von den Wörtern die Anfangsbuchstaben und ergänzen diese um Ziffern und Sonderzeichen. (Ein FC-Bayern-Fan könnte sich vielleicht mit *fCB!4ev* anfreunden.) Dazu kommt der jeweils spezifische Teil, der aus drei oder vier weiteren Zeichen besteht, die der Einfachheit halber aus dem Namen des Diensts abgeleitet sein können. Nehmen Sie also die beiden oder drei ersten oder letzten Buchstaben des Namens oder ersetzen Sie einen oder zwei Buchstaben davon durch Sonderzeichen oder Zahlen (etwa die Stelle des Alphabets, an der sich der jeweilige Buchstabe befindet). Ihrer Fantasie sind keine Grenzen gesetzt.

Haben Sie ein E-Mail-Konto bei GMX, könnten Sie das Passwort *gMXzN7m&!T* verwenden oder *g13XzN7m&!T* (M als 13. Buchstabe im Alphabet). Für Ihr Amazon-Konto könnte das Passwort entsprechend *aMAzN7m&!T* lauten oder eben *a13AzN7m&!T*. Auch bei nur selten genutzten Konten können Sie dann Ihr Passwort schnell wieder rekonstruieren. Und wenn Sie Ihrem Gedächtnis nicht völlig vertrauen, können Sie sich zumindest notieren, wie Sie die Kennwörter zusammengebaut haben. Durch die ständige Nutzung des abstrakten Passwortkerns und die ableitbare Passworterweiterung für die jeweiligen Dienste ist ein guter Kompromiss zwischen Sicherheit, Merkbarkeit und Praktikabilität gefunden.

Wenn Ihnen dies alles zu viel Mühe macht, können Sie auch Passwortgeneratoren einsetzen, die sichere Passwörter erzeugen. Allerdings werden dann zwar sichere Passwörter erstellt, einfach zu merken sind die Zeichenfolgen jedoch nicht. Neben eigenständigen Programmen wie PWGen gibt es auch Onlinegeneratoren, bei denen Sie allerdings auch wieder darauf vertrauen müssen, dass die Betreiber des Diensts die generierten Passwörter nicht selbst aufzeichnen und verwerten.

Wenn Sie ein sicheres Passwort erstellen möchten, können Sie sich von einem Generator helfen lassen.

Zwei-Faktor-Authentifizierung

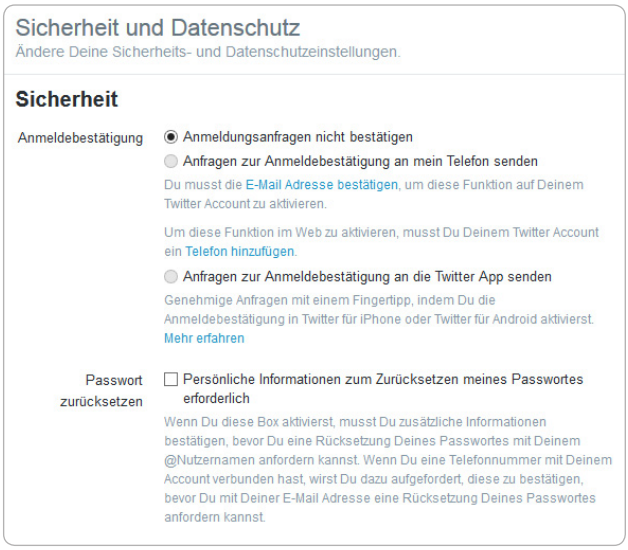
Mehr Schutz als ein einfaches Passwort bietet die Zwei-Faktor-Authentifizierung. Hinter diesem etwas sperrigen Begriff verbirgt sich ein im Grunde simpler Ansatz.

Bei der konventionellen Anmeldung dient ausschließlich das Passwort als Authentizitätsnachweis. Gelangt das Passwort in die Hände eines Dritten, kann sich dieser damit direkt anmelden. Bei der Zwei-Faktor-Authentifizierung kommt ein zweites Element hinzu. Dies kann beispielsweise ein körperliches Merkmal sein, das über biometrische Verfahren wie einen Fingerabdruckscan oder einen Irisscan ausgelesen wird. Eine Anmeldung über den Fingerabdrucksensor und eine PIN wäre eine solche Zwei-Faktor-Authentifizierung. Ein abgefangenes Passwort allein reicht nicht für den Identitätsdiebstahl aus.

Die Erfassung von Fingerabdrücken ist allerdings relativ aufwendig, und ein Irisscan ist nochmals komplizierter, daher werden meist andere Elemente als zweiter Faktor neben dem Passwort verwendet. Häufig kommt dabei das Smartphone zum Einsatz, über das ein zusätzlicher, zeitlich befristet gültiger Passcode per App oder SMS zugeschickt wird. Ein Smartphone oder Handy besitzt fast jeder und hat das Gerät ja auch fast immer dabei, sodass dieses Verfahren besonders praktisch ist. Die beiden Faktoren sind dann das Passwort (oder PIN) einerseits und der per Smartphone empfangene Passcode andererseits.

Es gibt auch erste Versuche, den zweiten Faktor über Hardwaretoken zu generieren, die Einmalpasswörter erzeugen. Ein solches Token kann ein Mini-USB-Stick sein, der zur Authentifizierung eingesteckt wird. Noch bequemer sind Token, die per NFC-Funktechnik drahtlos mit dem Tablet oder Smartphone kommunizieren. Diese Technik kann auch in Alltagsgegenstände wie Schlüsselanhänger oder Schmuck integriert werden. Als primärer Authentifizierungsfaktor kann eine PIN oder ein Passwort genutzt werden. Google plant derzeit eine Tokenlösung zur Anmeldung am Google-Konto. Es ist aber noch nicht absehbar, wann und ob dieses Verfahren tatsächlich zum Einsatz kommt.

Eine einfache Zwei-Faktor-Authentifizierung per Handy oder Smartphone bietet bereits der Kurznachrichtendienst Twitter an, bei dem Sie Ihre Mobilfunkrufnummer angeben können, um die Anmeldung durchzuführen. Auch Google, Dropbox und Microsoft arbeiten bereits mit dieser Methode, die optional zum einfachen Passwortverfahren angeboten wird.



Twitter bietet optional eine Zwei-Faktor-Authentifizierung an, um Missbrauch zu erschweren.

2.5 Bleiben Sie informiert

Die Bedrohungslage durch Schadsoftware ändert sich sehr schnell. In immer kürzeren Abständen entwickeln Hacker neue Varianten ihrer Schadprogramme. IT-Sicherheitsexperten entdecken immer wieder auch Schädlinge, die schon geraume Zeit im Umlauf waren, sich aber so gut tarnten, dass sie lange unentdeckt bleiben konnten.

Einen ähnlichen Wettlauf gibt es beim Phishing. Auch hier verfeinern Betrüger ihr Repertoire immer weiter und setzen auf neue Tricks und perfekt nachgemachte E-Mails oder gefälschte Webseiten. In jüngster Zeit wurden zahlreiche Phishing-Mails versendet, bei denen die Adressaten ganz persönlich mit ihren richtigen Namen angesprochen wurden. Die Phishing-Mails waren meist als Telekom-Rechnungen getarnt, und durch die persönliche Ansprache ließen sich viele Empfänger dazu verleiten, die vermeintliche Rechnung im Mailanhang zu öffnen, wodurch eine Schadsoftware auf den Rechner geladen wurde. Mittlerweile haben die Telekom und andere Unternehmen angekündigt, die Sicherheit ihrer E-Mails durch zusätzliche Maßnahmen zu erhöhen. So ist neben anderen Aktionen etwa geplant, bei echten Rechnungsmails der Telekom die Adresse der jeweiligen Empfänger in der Betreffzeile anzugeben, da diese Information bei den Hackern meist nicht vorhanden ist.

Informationsquellen

Um auf aktuelle Gefahren durch neu entdeckte Schadprogramme oder Schwachstellen in Programmen sowie neue Phishing-Angriffe unverzüglich reagieren zu können, müssen Sie zunächst einmal an die entsprechenden Informationen gelangen. Dabei hilft ein Besuch auf den Webseiten der großen IT-Sicherheitsanbieter oder auf deren Twitter- oder Facebook-Seiten.

Eine andere Informationsquelle sind die Onlineangebote der großen Computermagazine. Hier gehören die Sicherheitsseiten des Heise-Verlags zu den informativsten Angeboten, die zeitnah über neue Risiken berichten und auch umfassende Tipps geben, wie Sie Gefahren umgehen oder minimieren können.

Die Security-Seiten erreichen Sie unter der Webadresse *www.heise.de/security/*. Weitere unabhängige Informationsseiten sind:

- Spam-Info (*www.spam-info.de*)
- Mimikama (*www.mimikama.at*)

Sie sollten auch regelmäßig auf die Website des *Bundesamts für Sicherheit in der Informationstechnik* (BSI) schauen. Dort gibt es eine spezielle Seite, die neben vielen Grundlageninformationen aktuelle Warnhinweise bietet. Unter *www.bsi-fuer-buerger* finden Sie dieses Informationsangebot, und auch auf Facebook ist das BSI zu erreichen.

Eine andere wichtige Informationsquelle ist das Bürger-CERT. CERT steht für *Computer Emergency Response Team* und bezeichnet ein Team von Sicherheitsfachleuten, die mit ihrem Wissen anderen Anwendern zur Seite stehen. Auf der Website können Sie verschiedene Newsletter abonnieren, die über unterschiedliche Sicherheitsaspekte informieren. Es gibt z. B. einen regelmäßig erscheinenden Newsletter mit allgemeinen Informationen, der für Laien konzipiert und leicht verständlich ist.

Bei besonders gravierenden Sicherheitsproblemen wird dieses Angebot um Extraausgaben ergänzt. Des Weiteren gibt es noch einen Informationsdienst mit technischen Warnungen, der Hintergrundinformationen und konkrete technische Hilfestellungen liefert und sich vor allem an versierte Anwender richtet, die ein grundlegendes Know-how besitzen. Das Angebot des Bürger-CERT finden Sie unter der Adresse *www.buerger-cert.de*.

Das BSI informiert laufend über aktuelle Bedrohungen im Internet.

SICHERHEITSTIPPS IM ÜBERBLICK

- Verwenden Sie auf Windows-Rechnern und Android-Mobilgeräten eine Antivirensoftware.
- In konkreten Einzelfällen (z. B. bei einem verdächtigen Mailanhang) ist eine zusätzliche Überprüfung durch einen Onlinevirenscanner hilfreich.
- Aktualisieren Sie Betriebssystem und Anwendungen wenn möglich über automatische Updates (wie bei Windows) oder manuell.
- Deinstallieren Sie Anwendungen, die Sie nicht mehr benötigen. Überlegen Sie vor der Neuinstallation, ob Sie die Software tatsächlich benötigen.
- Überprüfen Sie per Onlinecheck Ihren Router auf Schwachstellen.
- Verwenden Sie WPA2 (oder WPA) für die WLAN-Verschlüsselung, keinesfalls mehr WEP.
- Ändern Sie das vom Hersteller voreingestellte WLAN-Passwort.
- Verwenden Sie ausschließlich sichere Passwörter, die den Mindestanforderungen entsprechen.
- Informieren Sie sich über die aktuelle Gefahrenlage.

Auch wenn die mobile Internetnutzung per App immer wichtiger wird, bleibt der Browser die wichtigste Software für das Web. Ebenso wird die immer wieder totgesagte E-Mail trotz der zunehmenden Konkurrenz durch Messenger und Chats noch lange Zeit das wichtigste Kommunikationsinstrument bleiben. Im folgenden Kapitel zeigen wir, wie Sie sich mit dem Browser im Web sicher bewegen und worauf Sie bei der Nutzung von E-Mail achten sollten. Bei den Sicherheitseinstellungen der Browser haben wir die drei populärsten Anwendungen Firefox, Chrome und Internet Explorer berücksichtigt.

3.1 Browsersicherheitseinstellungen

Im Web lauern Gefahren. Einige davon betreffen direkt die Sicherheit, wenn auf Webseiten gefährliche Schadprogramme verteilt oder auf nachgemachten Phishing-Webseiten Daten abgegriffen werden, bei anderen geht es »nur« um Angriffe auf Ihre Privatsphäre durch Cookies und andere Techniken, die Ihr Surfverhalten aufzeichnen oder andere persönliche Daten sammeln.

Gefahren durch aktive Inhalte im Web

Schon das Surfen kann gefährlich sein. Manchmal reicht bereits der Besuch einer Webseite, um den eigenen Rechner mit einer Schadsoftware zu infizieren. Sie müssen also nicht einmal eine Datei explizit herunterladen und öffnen, um den Schädling zu übertragen, schon beim Betrachten einer Webseite kann die Infektion passieren. Diese Drive-by-Downloads sind besonders gefährlich und werden leider immer häufiger eingesetzt.

Möglich werden diese Angriffe durch aktive Inhalte und dynamische Funktionen, bei denen der Browser eigenständig mit Servern kommuniziert und Dateien abruft. Techniken, die mit aktiven Inhalten arbeiten, sind JavaScript, Java, Flash und auch ActiveX, das nur vom Internet Explorer genutzt wird. Da sich ActiveX nicht als Standard etablieren konnte und der Internet Explorer auch keine herausragende Stellung auf dem Browsermarkt mehr einnimmt, spielt es kaum noch eine Rolle.

Auch Java wird immer seltener verwendet. Diese Entwicklung wird von Sicherheitsexperten sehr begrüßt, da sich die Java-Software in der Vergangenheit immer wieder als fehleranfällig und damit als Einfallstor für Schadsoftware herausgestellt hatte.

GEFAHREN LAUERN ÜBERALL

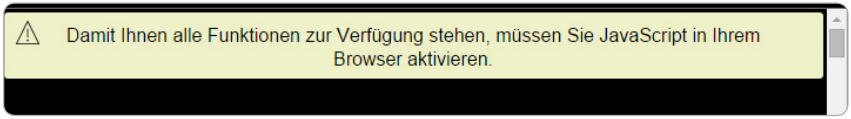
Die ersten Drive-by-Downloads gab es vor allem auf dubiosen Webseiten. Wer nach Softwareraubkopien suchte oder andere illegale Inhalte herunterladen wollte, musste damit rechnen, sich eine Schadsoftware einzufangen. Jetzt drohen die Gefahren auch auf ganz seriösen Seiten. Sind Webserver unzureichend gesichert, können sie gehackt und manipuliert werden, sodass auch völlig harmlose Seiten auf einmal eine Bedrohung darstellen. Besonders häufig erfolgen Drive-by-Downloads über multimediale Werbebanner, die auf Webseiten eingeblendet werden. Hier müssen Angreifer lediglich manipulierte Werbung auf den Servern der Werbehoster platzieren, die diese Elemente anschließend an die Websites ausliefern. Dadurch können Sie sich dann auch auf großen und renommierten Websites mit Schadsoftware infizieren.

Prüfen Sie, ob die Java-Version auf Ihrem Rechner aktuell ist.

JAVA IST KEIN MUSS MEHR

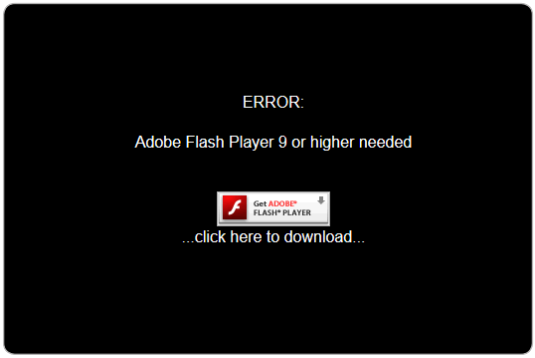
Sind Sie bislang ohne Java auf Ihrem Rechner ausgekommen, besteht kein Anlass, diese Software nachträglich zu installieren. Mittlerweile hat Java-Entwickler Oracle die Sicherheitsproblematik zwar besser im Griff, dennoch ist es fraglich, ob sich die Verwendung tatsächlich lohnt. Wenn Sie auf die Nutzung von Webseiten mit Java nicht verzichten wollen oder können, sollten Sie darauf achten, dass Sie über aktuelle Versionen der Plug-ins und des JRE (*Java Runtime Environment*) verfügen, um Risiken zu minimieren. Auf der Java-Website (*www.java.com/de/download/installed8.jsp?detect=jre*) können Sie überprüfen, ob auf Ihrem Rechner die aktuelle Version vorhanden ist.

Deutlich größer ist dagegen die Bedeutung von JavaScript. Es gibt nur sehr wenige Seiten, die nicht damit arbeiten. Für die Anzeige und Wiedergabe von JavaScript-Elementen benötigen Sie kein Plug-in oder irgendeine sonstige Erweiterung und auch keine Zusatzsoftware auf Ihrem Rechner, da Java von nahezu allen Browsern direkt unterstützt wird. Trotz der Namensähnlichkeit gibt es keine Gemeinsamkeiten zwischen Java und JavaScript. Die Ausführung von JavaScript lässt sich in den Browsern deaktivieren, was zwar die Sicherheit erhöht, andererseits aber eine normale Webnutzung weitestgehend verhindert.



Ohne JavaScript werden viele Seiten nicht korrekt angezeigt und sind kaum nutzbar.

Auch Flash kommt auf sehr vielen Webseiten zum Einsatz. Anders als bei JavaScript benötigen Sie jedoch eine Erweiterung für den Browser, um diese Elemente wiedergeben zu können. Entsprechende Add-ons gibt es für alle wichtigen Browser. Entwickelt wurde Flash von Adobe, es wird vor allem für Animationen, Videos und andere multimediale und interaktive Elemente auf Webseiten eingesetzt. Ohne Flash-Erweiterung sind viele Webseiten nur eingeschränkt nutzbar. Einige Browser wie Chrome und der Internet Explorer haben die Flash-Erweiterung bereits integriert, sodass kein Download notwendig ist.



Fehlt dem Browser das Flash-Plug-in, müssen Sie es nachinstallieren.

SICHERHEITSRISIKO FLASH

Leider hat sich Flash zu einem Haupteinfallstor für Drive-by-Downloads entwickelt, da auch hier immer wieder Schwachstellen entdeckt werden. Nicht immer gelang es Adobe, Sicherheitsupdates kurzfristig bereitzustellen, sodass Lücken mitunter längere Zeit offen blieben und aktiv für Angriffe ausgenutzt wurden. Auf jeden Fall sollten Sie immer mit der aktuellsten Version des Flash-Players ins Web gehen, allerdings ist die Aktualitätskontrolle etwas umständlich: Rufen Sie die Adobe-Webseite *www.adobe.com/de/software/flash/about/* auf, wird Ihnen angezeigt, welche Version Sie nutzen und welche die aktuelle Version ist.

Gefahren durch Phishing

Die zweite große Gefahrenquelle beim Surfen im Web sind Phishing-Webseiten. Dabei handelt es sich um gefälschte oder nachgestellte Webseiten, über die Betrüger Ihre Zugangsdaten abfangen wollen. Was also in Ihrem Browser aussieht wie die Anmeldeseite für das Onlinebanking oder die Startseite Ihres Webmail-Dienstleisters, ist bei einer solchen Attacke gar nicht das Original, sondern eine geschickte Imitation. Geben Sie dort Benutzername und Passwort in die Formularfelder für die Anmeldung ein, landen diese Informationen direkt bei den Betrügern, die sie weiterverwenden.

Über Phishing-Seiten versuchen Betrüger, an Ihre Zugangsdaten zu gelangen.

WOHIN FÜHRT DER LINK?

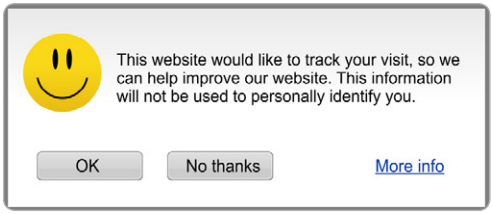
Beim Surfen im Web empfiehlt es sich – genau wie im Straßenverkehr –, vorausschauend zu handeln. Konkret bedeutet dies, dass Sie vor dem Anklicken eines Links einen Blick darauf werfen, wohin Sie dieser Klick führen wird. Ihr Browser zeigt Ihnen daher das Ziel des Links als Internetadresse (URL) an, wenn Sie den Mauszeiger auf dem Link platzieren. Die URL sehen Sie in der Statuszeile am unteren Bildrand oder in einer Einblendung. So erkennen Sie auf einen Blick, ob Sie die aktuelle Website verlassen, wenn Sie den Link anklicken. Meist ist auch ersichtlich, zu was für einer Art von Dokument (normale Webseite, PDF-Datei etc.) Sie gelangen, was wiederum Rückschlüsse auf mögliche unliebsame Überraschungen zulässt. Problematisch sind daher URL-Verkürzer, wie sie bei Twitter und ähnlichen Angeboten verwendet werden. Hier gibt es statt der echten URL nur ein Kürzel, das keine Informationen bietet. Für die meisten Browser gibt es daher Add-ons, die diese Kurzlinks wieder zurückübersetzen, sodass Sie erkennen können, welches Linkziel Sie erwartet. Diese Tools finden Sie bei Browser-Add-on-Angeboten unter dem Begriff *LongURL*.

Viele Browser besitzen einen Phishing-Filter, der solche Betrügereien verhindern soll. Der Filter arbeitet mit einer Liste der Webadressen verdächtiger Seiten, blendet eine Warnung ein und unterbindet den Zugriff, wenn Sie versuchen, sich mit einer verdächtigen Seite zu verbinden. Nebenbei werden auf diesem Weg auch Seiten blockiert, auf denen bekanntermaßen Schadsoftware verteilt wird.

Schutz der Privatsphäre

Schließlich gibt es noch einen dritten Aspekt bei der Browsernutzung, der weniger die Sicherheit als den Schutz Ihrer Privatsphäre betrifft. Gemeint ist der Umgang mit Cookies, mit denen Informationen auf Ihrem Rechner gespeichert werden können, und ähnlichen Techniken, mit denen Daten zum Nutzungsverhalten aufgezeichnet werden.

Cookies haben aber nicht nur negative Aspekte, sondern machen in vielen Fällen die Internetnutzung deutlich komfortabler und einfacher, indem sie personalisierte Dienste in die Lage versetzen, Besucher wiederzuerkennen und nur die Nachrichten anzuzeigen, die diese interessieren. Auch andere Anwendungen, wie Warenkorbsysteme in Onlineshops, nutzen Cookies.



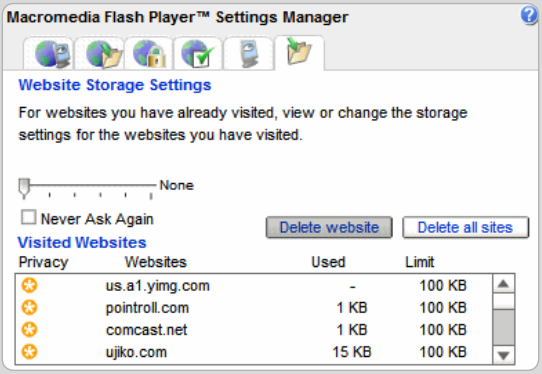
Immer mehr Seiten weisen auf die Verwendung von Cookies hin.

Eine Unterscheidung zwischen »guten« und »schlechten« Cookies ist daher nicht einfach. In allen Browsern gibt es detaillierte Einstellungsoptionen zu Cookies, allerdings steht der Aufwand für die Feinabstimmung meist in keinem Verhältnis zum Ergebnis, zumal es neben konventionellen Cookies auch andere Techniken gibt, mit denen Sie als Nutzer identifiziert werden.

FLASH-COOKIES

Eine besondere Art von Cookies wird bei der Nutzung von Flash gespeichert. Flash-Cookies werden von regulären Cookie-Filtern nicht erfasst. Sie können über den *Settings Manager*, der über das Internet erreichbar ist, nachsehen, welche Cookies auf Ihrem Rechner vorhanden sind, und diese einzeln oder komplett löschen. Die Adresse für den Einstellungsmanager lautet *www.macromedia.com/support/documentation/de/flashplayer/help/settings_manager07.html*. Dort können Sie weitere sicherheitsrelevante Einstellungen vornehmen, etwa zur Freigabe von Webcam und Mikrofon an Ihrem Rechner. ▸

FLASH-COOKIES *(FORTS.)*



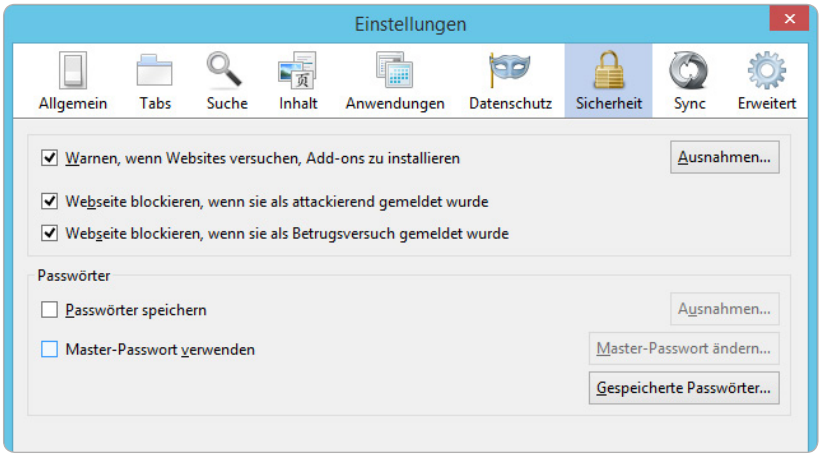
Über den Einstellungsmanager können Sie Flash-Cookies entfernen.

Sicherheit und Datenschutz bei Firefox

Der in Deutschland populärste Browser ist derzeit Firefox, der allerdings zuletzt Marktanteile an Google Chrome abgeben musste. Firefox zeichnet sich unter anderem durch übersichtliche Einstellungsoptionen in den Bereichen Sicherheit und Privatsphäre aus. Zu diesen gelangen Sie über die Menüschaltfläche oben rechts im Browserfenster und den Menüpunkt *Einstellungen*.

Die sicherheitsrelevanten Einstellungen wurden auf mehrere Register verteilt. Wichtig sind automatische Updates für den Browser. Die Einstellung dafür finden Sie im Bereich *Erweitert* auf der Registerkarte *Update*. Kontrollieren Sie dort, ob die Option *Updates automatisch aktualisieren* aktiviert ist, wenn nicht, holen Sie das nach. Sie müssen sich dann nicht mehr selbst um die Aktualisierung des Browsers kümmern.

Im Bereich *Sicherheit* sollten Sie darauf achten, dass die Optionen des integrierten Phishing-Filters (*Webseite blockieren, wenn sie als attackierend gemeldet wurde* und *Webseite blockieren, wenn sie als Betrugsversuch gemeldet wurde*) eingeschaltet sind. Ebenso sollten Sie sich einen Warnhinweis einblenden lassen, wenn Webseiten versuchen, Add-ons zu installieren. Auch von Add-ons könnten Sicherheitsgefahren ausgehen, sodass ohne Ihre Zustimmung keine Add-ons auf dem Rechner installiert werden sollten.

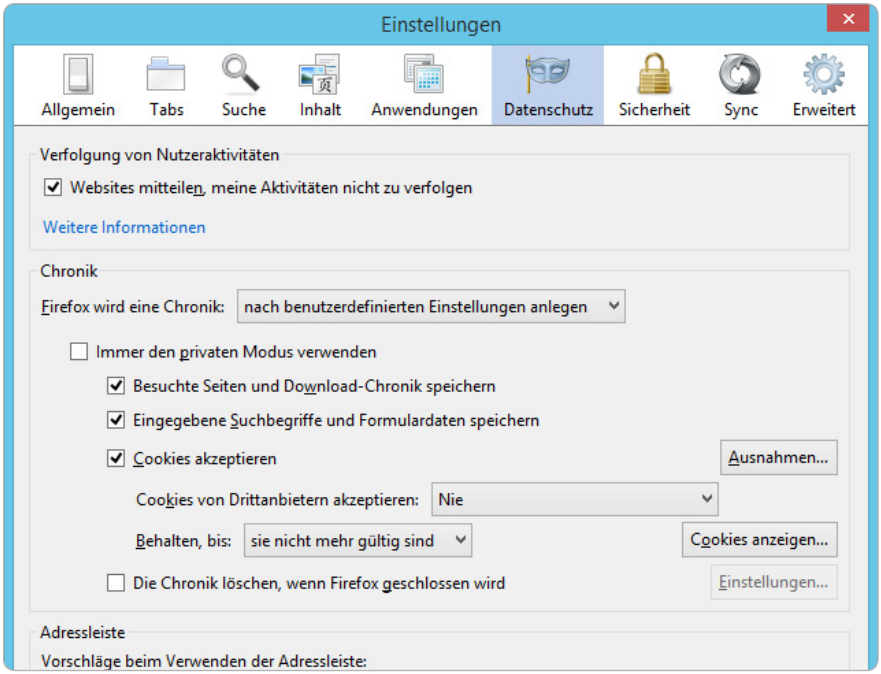


Die sicherheitsrelevanten Optionen in den Firefox-Einstellungen.

Sie können hier auch den Passwortspeicher von Firefox aktivieren, der Ihre Passwörter verschlüsselt speichert und auf den Anmeldeseiten automatisch einfügt. Zum Zugriff auf die Passwörter müssen Sie sich mit einem Masterpasswort legitimieren. Die Funktion ist sehr bequem, hat aber auch den Nachteil, dass Sie sich einzelne Passwörter wegen fehlender Nutzung nicht merken können und Probleme bekommen, wenn Sie sich von einem anderen Rechner aus anmelden möchten. Zudem sind gleich alle Ihre Onlinekonten in Gefahr, wenn das Masterpasswort in falsche Hände gerät. Auf dem heimischen PC ist dieses Risiko vielleicht noch akzeptabel, auf einem mobilen Rechner, der schnell abhandenkommen kann, kaum. Sie müssen selbst entscheiden, ob Sie die zusätzlichen Risiken lieber vermeiden möchten.

Im Register *Datenschutz* gibt es einen Bereich, der mit *Verfolgung von Nutzeraktivitäten* überschrieben ist. Hier legen Sie fest, ob Aktivitäten nicht verfolgt werden sollen, von den Websites doch verfolgt werden dürfen oder ob Sie dazu keine Vorgabe machen möchten. Hinter diesen Optionen verbirgt sich das *Do-not-Track-Verfahren*, das Webseiten beim Aufruf durch den Browser mitgeteilt, ob der Anwender dem Einsatz von Tracking-Mechanismen zustimmt oder nicht. Derzeit ist die Teilnahme am Do-not-Track-Verfahren für Webanbieter freiwillig geregelt und nicht verpflichtend. Sie können daher nicht sicher sein, ob Ihrem Wunsch, auf Überwachung zu verzichten, nachgekommen wird oder nicht. Allerdings schadet es auch nicht, wenn Sie die Option *Websites mitteilen, meine Aktivitäten nicht zu verfolgen* aktivieren.

Darunter haben Sie Einstellungsmöglichkeiten zur Chronik, in der der Verlauf der besuchten Webseiten gespeichert wird. Ein genereller Verzicht auf den Verlauf ist nicht anzuraten, da Sie dann Seiten, die Sie besucht haben, kaum noch wiederfinden können. Dennoch sollten Sie keine allgemeine Chronik nutzen, sondern im Fenster die Variante *Chronik nach benutzerdefinierten Einstellungen anlegen* auswählen. Erst dadurch haben Sie die Möglichkeit, auch einige grundlegende Cookie-Einstellungen vorzunehmen.



Die detaillierten Cookie-Einstellungsoptionen sind nicht direkt sichtbar.

Eine generelle Ablehnung aller Cookies ist nicht angebracht, da Cookies auch für durchaus wünschenswerte Zwecke verwendet werden.

Eine Kompromisslösung besteht darin, dass Sie Cookies immer nur so lange speichern, wie Firefox geöffnet bleibt. Mit dem Ende einer Surftour und dem Beenden von Firefox werden automatisch alle Cookies gelöscht. Davon sind dann allerdings auch die nützlichen und harmlosen Varianten betroffen.

COOKIES VON DRITTEN ABLEHNEN

Cookies von Drittanbietern sollten Sie ablehnen, da es sich dabei nahezu ausschließlich um Werbenetzwerke handelt, die Ihr Nutzungs- und Surfverhalten erfassen wollen, um Ihnen passgenaue Werbung einblenden zu können. Optional können Sie auch manuell festlegen, welche Websites Cookies anlegen dürfen und welche nicht. Allerdings ist die Erstellung einer solchen Liste mit erheblichem Aufwand verbunden und wenig praktikabel.

Einen positiven Effekt auf die Sicherheit kann auch der Pop-up-Blocker haben, der das Einblenden zusätzlicher Browserfenster blockiert. Sie aktivieren den Blocker im Register *Inhalt*. Sollten Sie auf vertrauenswürdigen Webseiten, die mit Pop-up-Fenstern arbeiten, diese Fenster zulassen wollen, können Sie dort auch eine Liste mit Ausnahmen anlegen.

Mehr Sicherheit mit Firefox-Add-ons

Für den Firefox gibt es eine ganz Reihe von Erweiterungen, mit denen Sie zusätzliche Funktionen nachrüsten können. Diese Zusätze werden bei Firefox Add-ons genannt und lassen sich ganz einfach dem Browser hinzufügen. Über *Einstellungen/Add-ons* gelangen Sie zu einer Übersicht der installierten Erweiterungen, können über *Add-ons suchen* auch auf die Add-on-Website wechseln und in verschiedenen Kategorien nach weiteren Ergänzungen suchen. Dort gibt es in der Rubrik *Datenschutz & Sicherheit* auch viele Sicherheitserweiterungen. Am populärsten sind Werbeblocker und Tools, mit denen Sie anonym surfen können. Im Hinblick auf die Sicherheit gehört NoScript zu den beliebtesten Angeboten.

NOSCRIPT SCHÜTZT VOR AKTIVEN INHALTEN

NoScript soll die automatische Ausführung von aktiven Inhalten verhindern und blockiert JavaScript, Java-Applets, Flash und Silverlight. Silverlight ist die Microsoft-Alternative zu Flash und Java, für die die meisten Browser ein Plug-in zur Ausführung benötigen. Darüber hinaus schützt NoScript auch vor *Cross-Site-Scripting* (kurz XSS). Gemeint sind damit Angriffe, bei denen Schwachstellen auf Webservern genutzt werden, um fremde Inhalte in Webseiten einzubauen, über die Nutzerdaten per Phishing abgefangen werden können. Auch Schadcode kann über solche XSS-Attacken verteilt werden.

Das Sperren dieser Inhalte (insbesondere der weitverbreiteten JavaScript- und Flash-Elemente) macht allerdings die allermeisten Webseiten weitgehend unbrauchbar. Deshalb bietet NoScript die Option, Ausnahmen zuzulassen. Diese Ausnahmen können in unterschiedlicher Form erteilt werden.

Zum einen können Sie die Ausnahmegenehmigungen nur für den aktuellen Seitenbesuch bis zum Schließen des Browsers erteilen (temporäre Erlaubnis), zum anderen können Sie diese Ausnahmen auch dauerhaft speichern, sodass Ihnen bei späteren Besuchen die Webseite gleich richtig angezeigt wird und der volle Funktionsumfang nutzbar ist. Auf diese Weise erstellen Sie im Lauf der Zeit eine umfangreiche »weiße Liste« mit Ausnahmen, sodass sich der Komfortverlust durch NoScript in Grenzen hält.

Auf vielen Seiten ist eine Fülle von aktiven Elementen aus unterschiedlichen Quellen zu finden.

Problematisch ist allerdings, dass auf vielen Webseiten nicht nur Skripte und aktive Inhalte laufen, die vom ursprünglichen Server des Anbieters kommen, sondern häufig auch viele Elemente von externen Servern stammen. Auf einigen Webseiten finden sich Dutzende externer Elemente. Von diesen externen Komponenten werden einige für die Einbindung zusätzlicher Inhalte benötigt, sodass auch sie für die uneingeschränkte Nutzung der Webseite freigegeben werden müssen. Andere Inhalte sind hingegen unerwünscht, da sie etwa Tracking-Funktionen haben oder aufdringliche Werbung einblenden. Mit jedem zusätzlich freigegebenen Skript steigt auch das Risiko, dass Schadsoftware auf den Rechner gelangt.

Die Unterscheidung zwischen notwendigen und unerwünschten Elementen ist leider nicht immer einfach, denn in der NoScript-Liste sind nur die Namen der Server aufgeführt, die nicht immer einen Rückschluss darauf zulassen, um welche Art von Skript es sich handelt. Prinzipiell empfiehlt es sich daher, schrittweise vorzugehen und einzelne Server zunächst temporär freizugeben. Wird die Seite anschließend in gewünschter Weise angezeigt und kann in vollem Umfang genutzt werden, muss die Ausnahme nur noch dauerhaft gespeichert werden. Ist das nicht der Fall, müssen Sie weitere Server freigeben.

Da auch die meisten aufdringlichen Werbeeinblendungen und Tracking-Tools über Skripte funktionieren, hat NoScript nebenbei noch einen ähnlichen Effekt wie ein Werbeblocker, da es viele aufdringliche Werbebanner ebenfalls blockiert.

Sicherheit und Datenschutz bei Chrome

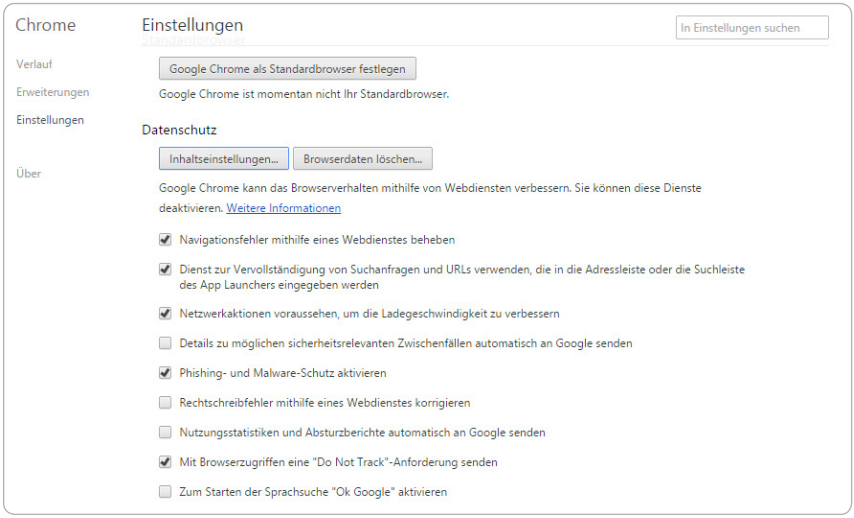
Der Google-Browser Chrome hat deutlich an Marktanteilen hinzugewonnen, was vor allem an der einfachen Bedienbarkeit liegen dürfte. Sicherheitsupdates werden hier beispielsweise völlig automatisch installiert, Anwender bekommen davon so gut wie gar nichts mehr mit.

Die Einstellungsoptionen sind bei Chrome übersichtlich. Sie erreichen sie über die Menüschaltfläche, die sich rechts neben dem Adresseingabefeld befindet. Im Menüfenster klicken Sie auf *Einstellungen*. Die sicherheitsrelevanten Optionen rufen Sie über *Erweiterte Einstellungen anzeigen* auf.

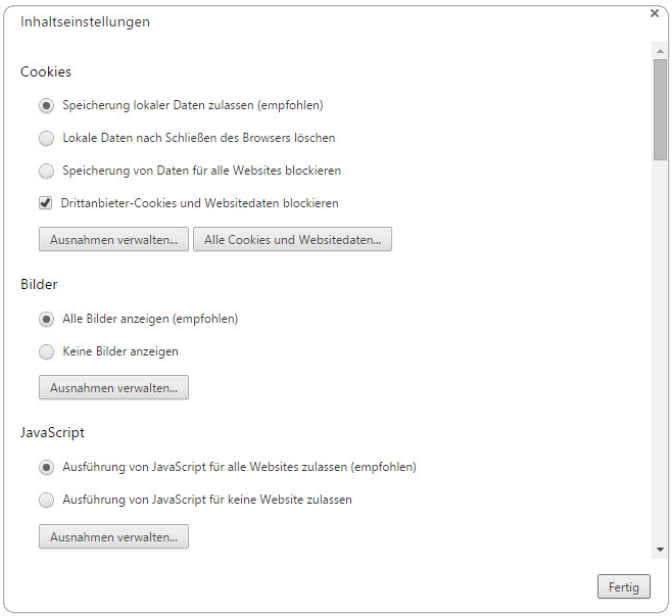
In diesen erweiterten Einstellungen gibt es wie bei Firefox eine Do-not-Track-Funktion, die bei Chrome standardmäßig abgeschaltet ist. Der tatsächliche Nutzen dieser Funktion ist derzeit noch gering, sodass es Ihnen überlassen bleibt, ob Sie sie einschalten oder deaktiviert lassen möchten.

In jedem Fall eingeschaltet sein sollte dagegen der integrierte *Phishing- und Malware-Schutz*. Dieser Schutz funktioniert wie bei den anderen Browsern und basiert auf einer Datenbank, in der verdächtige Webadressen gesammelt werden. Vor dem Aufruf einer Seite erfolgt ein Abgleich. Ist die Adresse in der Blacklist enthalten, wird ein Hinweis eingeblendet und der Aufruf blockiert.

Auch bei Chrome haben Sie die Möglichkeit, Webpasswörter zu speichern und mit einem Masterpasswort abzusichern. Ebenso können Sie eine Ausfüllhilfe aktivieren, mit der Angaben wie Name, Adresse, E-Mail-Anschrift etc. beim Eintragen in Webformulare automatisch ergänzt werden. Sie müssen



Die sicherheitsrelevanten Einstellungen finden Sie unter *Erweiterte Einstellungen*.



Im Bereich *Datenschutz* können Sie Vorgaben zu *Cookies* und *JavaScript* machen.

allerdings wieder daran denken, dass sich dadurch das Missbrauchsrisiko erhöht, wenn andere Personen Zugang zu Ihrem Rechner haben. Im Zweifelsfall deaktivieren Sie diese Optionen und verzichten auf den Komfort.

Das Cookie-Management von Chrome erreichen Sie über die Schaltfläche *Inhaltseinstellungen* im Bereich *Datenschutz*. Auch hier haben Sie die Möglichkeit, Cookies generell abzulehnen oder zu erlauben. Außerdem können Sie festlegen, dass Cookies nur temporär gespeichert und nach Schließen des Browsers automatisch gelöscht werden. Schließlich gibt es noch die Option zum gezielten Blockieren von *Drittanbieter-Cookies und Websitedaten*.

In diesem Fenster haben Sie auch die Möglichkeit, JavaScript generell zu blockieren, wobei es aber möglich ist, Ausnahmen zu machen. Sowohl bei der Blockade von Cookies als auch von JavaScript erscheint beim Aufruf einer Webseite mit derartigen Elementen ein Symbol in der Adressleiste, über das Sie Ausnahmen sehr einfach festlegen können.

NUTZEN SIE ERWEITERUNGEN FÜR CHROME

Auch für Chrome gibt es eine große Palette an Erweiterungen für unterschiedlichste Zwecke. Erweiterungen für Sicherheit und Datenschutz finden Sie im Chrome-Webstore unter der Rubrik *Produktivität*. Dort steht Ihnen beispielsweise ScriptSafe zur Verfügung, das zwar eine ähnliche Funktionalität besitzt wie NoScript für Firefox, jedoch nicht denselben Bedienungskomfort bietet.

Zertifikate in den Browsern überprüfen

Beim Aufruf von Webseiten, auf denen Sie sensible Daten eingeben, sollten Sie besonders wachsam sein. Wenn Sie sich also auf der Website Ihrer Onlinebank anmelden oder einen Onlinezahlungsdienst verwenden, sich bei Ihrem E-Mail-Postfach anmelden, in einem Onlineshop einkaufen oder sich bei anderen Onlinediensten einloggen, achten Sie darauf, dass Ihre Daten bei der Übertragung geschützt sind und Sie sich tatsächlich auf den Originalseiten befinden und nicht auf nachgestellten Phishing-Seiten.

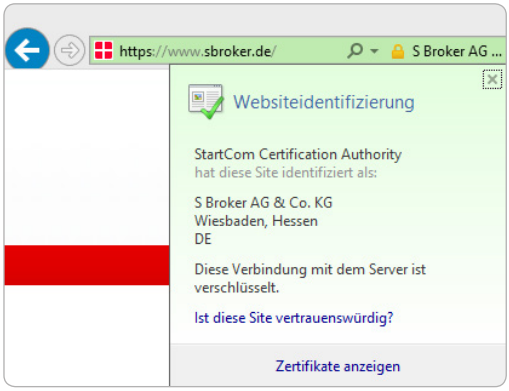
Sicherheit gibt Ihnen die SSL-Verschlüsselung, bei der die Daten nicht nur durch Verschlüsselung vor Abhörangriffen während der Übertragung geschützt werden, sondern Sie auch die Echtheit der Webseite überprüfen können, indem Sie

sich das Zertifikat der Webseite anzeigen lassen. Ein solches Zertifikat ist eine Art digitaler Ausweis, mit dem sich die Identität einer Website kontrollieren lässt.

SO ERKENNEN SIE SICHERE VERBINDUNGEN

Zu erkennen ist eine SSL-Verbindung bereits am Kürzel *https* anstelle des sonst üblichen *http* in der Adresszeile. Meistens wird in der Adresszeile auch noch das Symbol eines geschlossenen Vorhängeschlosses eingeblendet. Die meisten Browser färben bei SSL-Verbindungen dieses Symbol oder die Adresse grün ein, um Sicherheit zu signalisieren. Allerdings können Sie sich mittlerweile auf diese Anzeigen nicht mehr unbedingt verlassen, da auch professionelle Betrüger ihre Server mit Zertifikaten ausrüsten und Schwachstellen in der Überprüfung nutzen, die auch nachgemachte Webseiten vertrauenswürdig erscheinen lassen. Sie sollten daher bei sehr sicherheitsrelevanten Diensten nicht nur auf die *https*-Verbindung achten, sondern sich zusätzlich die Zertifikate anschauen.

Um ein Zertifikat zu kontrollieren, klicken Sie bei Internet Explorer und Firefox in der Adresszeile auf das Vorhängeschlosssymbol oder die farblich hervorgehobene Adresse. Sie bekommen erste wichtige Angaben zum Inhaber des Zertifikats und dem Aussteller angezeigt. Wenn Diskrepanzen zwischen dem Website-Betreiber und dem angegebenen Zertifikatsinhaber auftreten, sollten Sie vorsichtig bleiben. Sie können zusätzlich detailliertere Informationen zum Zertifikat abrufen, etwa wie oft Sie diese Webseite bereits besucht haben. Wenn es dann immer noch Unklarheiten gibt, sollten Sie den Besuch der Website abbrechen und sich an anderen Stellen über mögliche Sicherheitsprobleme informieren.



Sie sollten sich die Zertifikatsinformationen genauer ansehen.

Bei Chrome erhalten Sie nach dem Anklicken des SSL-Symbols in der Adresszeile eine allgemeine Übersicht über Berechtigungen, die dieser Webseite eingeräumt sind. Zudem wird angezeigt, ob das Zertifikat als sicher eingestuft wird. Für detailliertere Informationen zum Zertifikat klicken Sie in der Übersicht auf *Verbindungen*.

3.2 E-Mail-Sicherheit

E-Mail gehört trotz der zunehmenden Konkurrenz durch andere Kommunikationsmöglichkeiten im Internet (Chats, Messenger etc.) immer noch zu den unverzichtbaren Essentials bei der Internetnutzung. Allerdings ist E-Mail aus verschiedenen Gründen etwas in Verruf geraten, wobei auch Sicherheitsaspekte eine wesentliche Rolle gespielt haben.

So ist E-Mail schon immer ein populärer Übertragungsweg für Schadprogramme gewesen. Die Gefahr geht dabei nicht von den E-Mails selbst aus, sondern von den Dateianhängen. Das einfache Lesen einer E-Mail ist nicht kritisch, brisant wird es erst, wenn Sie auf den Dateianhang klicken. Dann kann es allerdings schon zu spät sein, weil ein Trojaner oder ein anderer Schädling Ihren Rechner vielleicht bereits infiziert hat.

Die zweite direkte Gefahr bei der E-Mail-Nutzung ist das Phishing. Hier wird kein verseuchter Dateianhang mitgeschickt, stattdessen möchte die E-Mail Sie auf eine Webseite leiten, auf der Sie persönliche Daten wie Passwörter, PIN und TANs sowie Informationen eingeben sollen. Manchmal sollen Sie auch auf Seiten geleitet werden, die Schadsoftware verteilen, über die Sie anschließend ausspioniert oder Ihr Rechner ferngesteuert werden kann. Insofern verschwimmen die Grenzen zwischen Phishing und der traditionellen Verteilung von Schadsoftware.

Keine direkte Gefahr, aber ein erhebliches Ärgernis ist E-Mail-Spam, unerwünschte Werbung per E-Mail für meist ohnehin dubiose Produkte oder Dienstleistungen. Der Anteil von Spam am gesamten E-Mail-Aufkommen ist erschreckend hoch: Mehr als 90 Prozent aller E-Mails sind Spam. Ein Großteil wird mittlerweile schon frühzeitig auf dem Übertragungsweg aussortiert, sodass in den E-Mail-Postfächern nur noch eine vergleichsweise geringe Zahl von Spam-Mails ankommt, allerdings ist auch hier der Spam-Anteil immer noch sehr hoch.

amazon.de

Guten Tag,

In den letzten Jahren ist die Zahl von Betrugsfällen auch bei Amazon nicht unbemerkt geblieben. Aus diesem Grunde rüsten wir unser Sicherheitssystem auf, um es den Betrügern unmöglich zu machen. Seit Neuestem setzen wir auf das sehr moderne "Verified by Visa" und "Mastercard SecureCode" Sicherheitsverfahren.

Um die Umrüstung auf das neue Sicherheitsverfahren problemlos gestalten zu können, bitten wir Sie im Vorraus Ihre Kreditkarten-Daten im Zusammenhang mit "Verified by Visa" bzw. "MasterCard SecureCode" zu ergänzen, um weiterhin wie gewohnt bei Amazon.de einkaufen zu können.

Der gesamte Prozess dauert nur wenige Minuten und ist mit keinerlei Kosten verbunden.

Zum Formular (über den Sicherheitsserver)

Ihre Daten werden vertraulich behandelt und nicht an Dritte weitergegeben.

Freundliche Grüße

Kundenservice Amazon.de
http://amazon.de

Beim Phishing sollen Sie unter einem Vorwand geheime Zugangsdaten preisgeben.

SCHUTZ VOR SPAM IST AUCH SCHUTZ VOR PHISHING UND E-MAIL-SCHADSOFTWARE

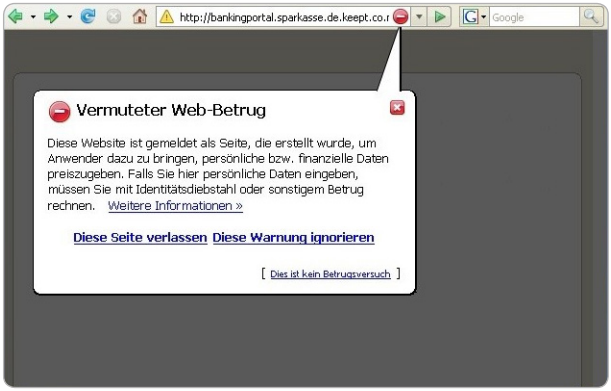
Spam stellt in gewisser Weise doch ein Sicherheitsrisiko dar, da auch die Versender von Phishing-Mails und Schadsoftware die E-Mail-Adressen der Empfänger benötigen. Diese bekommen sie von anderen Spam-Versendern und aus denselben Quellen, aus denen sich auch die Spam-Versender bedienen. Wer sich also erfolgreich vor Spam schützen kann, ist damit zugleich vor den meisten Phishing- und Malware-Mails sicher.

Beim Thema E-Mail geht es auch um die Sicherheit und Vertraulichkeit der übertragenen Informationen. E-Mail wird in immer mehr Alltagsbereichen verwendet, doch kaum jemand macht sich bewusst, dass eine E-Mail auf dem Übertragungsweg komplett ungeschützt ist und Inhalte genauso einfach von Dritten mitgelesen werden können wie Texte auf einer Postkarte. Außerdem gibt es weitere Sicherheitsprobleme – so lassen sich Absenderangaben sehr einfach fälschen, was sich Betrüger zunutze machen und durch Angabe einer seriösen Absenderangabe das Vertrauen potenzieller Opfer erschleichen.

Schutz vor Phishing und Schadsoftware in E-Mails

Den technischen Schutz vor Phishing und Schadsoftware übernehmen Browser und Antivirenprogramme. Die Antivirensoftware überprüft eingehende E-Mails und schlägt Alarm, wenn sich in einem Dateianhang ein Schädling versteckt. Der Phishing-Filter des Browsers sollte vor dem Aufruf einer in einer E-Mail verlinkten Webseite warnen, wenn diese Schadsoftware verteilt oder Nutzerdaten abfängt.

Leider erweisen sich die Schutzmaßnahmen in der Praxis jedoch nicht immer als zuverlässig, sodass es Schädlingen häufiger gelingt, sich an der Kontrolle vorbeizuschmuggeln. Bei Phishing-Filtern ist es ähnlich, allerdings ist die Erkennungsquote deutlich niedriger als bei Antivirensoftware, da Phishing-Webseiten vergleichsweise einfach einzurichten sind. Betrüger steigen mit ihren nachgestellten Seiten immer wieder auf neue Adressen um, sodass die Schutzlisten nicht im selben Tempo aktualisiert werden können.



Phishing-Filter bieten nur einen begrenzten Schutz.

BLEIBEN SIE WACHSAM

Sie können nie sicher sein, dass das Öffnen eines Dateianhangs nicht doch eine Schadsoftware installiert oder Sie beim Anklicken eines Links in einer E-Mail nicht doch auf eine Phishing-Webseite gelangen. Sie müssen daher immer wachsam bleiben und im Zweifelsfall auf das Öffnen eines Dateianhangs oder das Anklicken eines Links verzichten.

Erst nachdenken, dann klicken

Bei vielen Phishing-Angriffen hilft schon der gesunde Menschenverstand. Wenn Sie eine Gewinnmitteilungen erhalten, ohne an einem Gewinnspiel teilgenommen zu haben, sollte Ihnen das zu denken geben. Auch wenn sich Onlinebanken oder Zahlungssysteme bei Ihnen melden, bei denen Sie gar kein Konto haben, sollten Sie diese Nachrichten sofort ungesehen löschen.

Häufig versuchen Betrüger, Empfänger durch Einschüchterung zum Öffnen von verseuchten Dateianhängen zu bewegen. Es werden Rechnungen oder Mahnbescheide als Anhang gesendet, und E-Mails tarnen sich als Forderungen von Inkasso-Unternehmen oder gar als polizeiliche Anhörungsunterlagen. Oft wird aber auch eine gegenteilige Strategie verwendet, und E-Mails versprechen finanzielle Vorteile wie Steuerrückzahlungen oder Gutschriften von Onlineshops. Gerne nutzen Betrüger auch aktuelle Ereignisse und versprechen Dateien mit spektakulären Promifotos.

In all diesen Fällen sollten Sie die E-Mails ignorieren oder besser gleich löschen, sodass Sie nicht aus Versehen später noch die Dateianhänge anklicken.

Nicht immer sind spektakuläre Anlässe, Drohungen oder Belohnungen im Spiel, oft tarnen sich betrügerische E-Mails auch als einfache Telefonrechnung oder Benachrichtigung eines Paketdiensts. Dann ist es umso schwerer, die Betrugsabsicht zu erkennen. Wenn diese E-Mails auch noch optisch den Originalen gleichen und inhaltlich und sprachlich dem entsprechen, was zu erwarten ist, können selbst Experten manchmal nicht mehr unterscheiden, was eine gefährliche Phishing-Mail ist und was eine ganz legitime E-Mail eines Unternehmens.

SEHEN SIE SICH DIE HEADER-INFORMATIONEN AN

Da Absenderangaben bei E-Mails leicht gefälscht werden können, sollten Sie in Zweifelsfällen einen Blick auf die Header-Daten der E-Mail werfen. Am Header können Sie zwar den Absender nicht direkt erkennen, aber Unstimmigkeiten entdecken. So sind in den Header-Angaben unter dem Punkt *Received* die IP-Adresse des Absenders und der Name des E-Mail-Servers enthalten, von dem die E-Mail tatsächlich abgeschickt wurde. Gibt es zwischen der angegebenen Absenderadresse und dem tatsächlich genutzten E-Mail-Server Diskrepanzen, sollten Sie besonders vorsichtig sein.

Auch in Webmailern können Sie sich die Header-Informationen der E-Mails anzeigen lassen.

Wenn Sie nicht sicher sind, ob ein Dateianhang tatsächlich harmlos ist, können Sie auch eine Internetsuche mit dem Dateinamen starten. Eventuell gibt es ja schon erste Berichte zu einer Malware-Attacke, die diese Tarnung verwendet. Untersuchen Sie die Datei gezielt mit Ihrem Antivirenprogramm und lassen Sie sie zusätzlich durch einen Onlinevirenscanner untersuchen. Schließlich kann es auch hilfreich sein, zunächst einige Tage zu warten, denn viele Antivirenprogramme erkennen neue Schädlinge erst mit einiger Verzögerung.

SCHAUEN SIE SICH AKTUELLE PHISHING-WARNUNGEN AN

Phishing-Mails lassen sich immer schwerer erkennen. Über aktuelle Varianten können Sie sich auf dem Phishing-Radar der Verbraucherzentrale NRW informieren. Hier finden Sie nicht nur weitergehende Informationen zu betrügerischen E-Mails, sondern auch tagesaktuelle Meldungen. Die Seite erreichen Sie unter *www.vz-nrw.de/phishing* oder auf Twitter (*twitter.com/vznrw_phishing*).

SCHAUEN SIE SICH AKTUELLE PHISHING-WARNUNGEN AN *(FORTS.)*

Informieren Sie sich auf dem Phishing-Radar über die neuesten Varianten.

Tipps zur Vermeidung unerwünschter E-Mails

Damit Betrüger Sie mit Phishing-Mails und virenverseuchten Dateianhängen belästigen können, müssen sie an Ihre E-Mail-Adresse gelangen. Normalerweise kaufen sie genau wie Spam-Versender Listen mit Abertausenden oder gar Millionen von E-Mail-Adressen, die Adresssammler für wenig Geld anbieten.

Wenn Ihre E-Mail-Adresse gar nicht erst auf diese Listen gerät, bleiben Sie nicht nur von unerwünschten, sonst aber harmlosen Werbemails verschont, sondern bekommen auch keine gefährlichen E-Mails zugestellt. Die Erfassung Ihrer E-Mail-Adresse können Sie allerdings nur sehr bedingt verhindern.

Empfehlungen zur Spam-Vermeidung laufen darauf hinaus, dass Sie vorsichtig mit Ihrer E-Mail-Adresse umgehen. Die Veröffentlichung in Foren oder auf ähnlichen Webangeboten ist äußerst riskant, weil dort maschinell nach E-Mail-Adressen gesucht wird, und auch auf Webseiten ernten »Robots« Mailanschriften, sodass hier eine Veröffentlichung ebenfalls kritisch ist.

Auch die Teilnahme an Gewinnspielen und ähnlichen Aktionen ist wenig empfehlenswert, da Sie dann ja auch Ihre E-Mail-Adresse angeben. Zwar sind Anbieter verpflichtet, Sie in einer Datenschutzerklärung zu informieren, was mit Ihren Angaben geschieht, doch nicht immer geht daraus hervor, wer an Ihre Daten kommen kann. Außerdem hält sich nicht jeder Anbieter an diese Angaben.

ZAHLEN SIE NICHT MIT IHRER E-MAIL-ADRESSE

Bei Gratisangeboten im Web sollten Sie skeptisch sein, denn letztlich müssen Sie in irgendeiner Weise doch zahlen, und sei es durch die Preisgabe Ihrer E-Mail-Adresse, die durchaus einen, wenn auch geringen, Wert darstellt.

Die völlige Geheimhaltung Ihrer E-Mail-Adresse ist aber auch nicht der Weisheit letzter Schluss, schließlich möchten Sie per E-Mail mit anderen kommunizieren. Eine Veröffentlichung lässt sich daher nicht immer verhindern, und auch bei der Kontaktaufnahme mit Firmen oder anderen Organisationen im Web können Sie Ihre Mailanschrift ruhig weitergeben. Bei normaler Nutzung lässt es sich aber nicht vollständig ausschließen, dass Ihre E-Mail-Adresse in die Hände von Spam-Versendern gerät.

VERWENDEN SIE MEHRERE E-MAIL-ADRESSEN

Eine akzeptable Kompromisslösung ist es, mehrere E-Mail-Adressen zu verwenden. Neben einer privaten Adresse, die Sie nur sehr vorsichtig weitergeben und nach Möglichkeit niemals auf Webseiten öffentlich machen, nutzen Sie einfach eine zweite Adresse für all die Gelegenheiten, bei denen Sie um die Preisgabe nicht herumkommen. In diesem Postfach wird auch Spam landen, und darunter werden Phishing-Mails und Mails mit virenverseuchten Anhängen sein. Beim Öffnen der E-Mails aus diesem Postfach sollten Sie daher besonders vorsichtig sein.

Erkennbare Spam-Mails sollten Sie nach Möglichkeit gar nicht öffnen, da darin auch Bilder mit Webbugs enthalten sein können. Damit können Spam-Versender in Erfahrung bringen, ob und wann die E-Mail geöffnet wurde. Auf diese Weise können sie erkennen, ob ein E-Mail-Postfach überhaupt genutzt wird, und diese aktiven Mailkonten mit noch mehr Spam bombardieren.

BLOCKIEREN SIE BILDER

Viele E-Mail-Programme und Webmail-Angebote können so eingestellt werden, dass Bilder in E-Mails zunächst nicht heruntergeladen werden, um ein Ausspionieren zu verhindern. Sie sollten daher von diesen Optionen Gebrauch machen. Bilder von vertrauenswürdigen Absendern können Sie bei Bedarf ganz einfach nachträglich laden.

Auf Spam-Mails sollten Sie generell nicht reagieren. Auch wenn Links oder Antwortadressen zum Abmelden enthalten sind, sollten Sie sie nicht anklicken. Diese Reaktion zeigt den Spam-Versendern nur wieder, dass diese Mailadresse aktiv genutzt wird.

E-Mail-Verschlüsselung

Für das Problem der ungeschützten E-Mail-Kommunikation steht schon seit Langem eine Lösung bereit, die jedoch bis heute mit erheblichen Akzeptanzproblemen zu kämpfen hat. Die Lösung ist eine Verschlüsselung, die im Idealfall in einer Ende-zu-Ende-Version genutzt wird. Eine Ende-zu-Ende-Verschlüsselung ist dadurch gekennzeichnet, dass sie direkt beim Absender erfolgt und die Entschlüsselung erst beim Empfänger möglich ist. Auf dem gesamten Übertragungsweg, also auch auf den Servern der E-Mail-Provider, können die Daten nicht entschlüsselt werden.

Die Funktionsweise dieser Verschlüsselungstechnik ist recht einfach. Nachrichten, die mit dem öffentlichen Schlüssel eines Teilnehmers verschlüsselt werden, können ausschließlich mit dem dazugehörigen privaten Schlüssel wieder lesbar gemacht werden. Die beiden Schlüssel ergänzen sich, dennoch ist es unmöglich, aus dem öffentlichen Schlüssel den geheimen privaten Schlüssel herzuleiten.

VERSCHLÜSSELUNG IST SCHON LANGE MÖGLICH

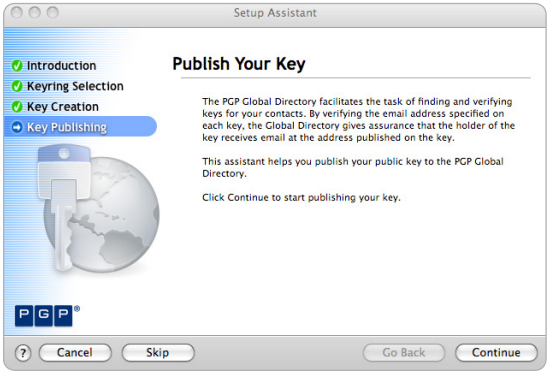
Speziell für E-Mail gibt es Ende-zu-Ende-Verschlüsselungslösungen schon seit vielen Jahren. Die bekanntesten Varianten sind PGP und S/MIME, die beide auf asymmetrischer Verschlüsselungstechnik basieren. Beide arbeiten mit einem Schlüsselpaar, das aus einem öffentlichen und einem privaten Schlüssel besteht. Der öffentliche Schlüssel wird den Kommunikationspartnern mitgeteilt, also öffentlich bekannt gemacht, der private Schlüssel bleibt dagegen geheim.

Um jemandem eine verschlüsselte Nachricht zukommen zu lassen, benötigt der Absender dessen öffentlichen Schlüssel. Mit diesem verschlüsselt er die Nachricht, und einzig und allein der Empfänger, der im Besitz des passenden privaten Schlüssels ist, kann den Inhalt wieder lesbar machen. Ohne diesen Schlüssel kann die Nachricht nicht gelesen werden.

Mit diesen Schlüsseln können E-Mails nicht nur verschlüsselt, sondern auch digital unterschrieben (signiert) werden. Die digitale Unterschrift wird erstellt, indem aus dem Inhalt der Nachricht eine Prüfsumme errechnet und mit dem privaten Schlüssel des Absenders verschlüsselt wird. Beim Empfänger wird die Prüfsumme mit dem öffentlichen Schlüssel wieder entschlüsselt und mit der erneut berechneten Prüfsumme der Nachricht verglichen. Stimmen beide Ergebnisse überein, ist sichergestellt, dass die Nachricht tatsächlich vom angegebenen Absender stammt und während der Übertragung nicht verändert wurde.

Damit die verschlüsselte Kommunikation in der Praxis funktionieren kann, muss sichergestellt werden, dass derjenige, der ein bestimmtes Schlüsselpaar nutzt, tatsächlich derjenige ist, für den er sich ausgibt. Denn prinzipiell wäre es ja jedem Anwender möglich, sich mehrere Schlüsselpaare anzufertigen und dann beispielsweise im Namen anderer Personen oder Institutionen zu agieren.

Die Bindung von Schlüssel und Inhaber erfolgt über Zertifikate. Ein Zertifikat bestätigt, dass der Inhaber eines öffentlichen Schlüssels tatsächlich derjenige ist, für den er sich ausgibt. Es ist also so eine Art digitaler Ausweis. Diese Bestätigung erfolgt durch den Zertifikatsherausgeber, der dazu die Identität des Antragstellers überprüft.



Die Verteilung und Verwaltung von Schlüsseln ist immer noch recht umständlich.

In der Praxis erweisen sich Verschlüsselungslösungen immer noch als recht kompliziert. Zertifizierung, Schlüsselverwaltung und Schlüsselverteilung sind Anforderungen, die viele Anwender abschrecken. Zudem sind die Verfahren nicht auf allen Endgeräten und Plattformen verfügbar, was angesichts der zunehmenden Nutzung von Tablets und Smartphones kaum noch akzeptabel ist. Einfache Lösungen, bei denen Nutzer mit diesen Prozessen kaum noch in Berührung kommen und E-Mails mit ein paar Klicks ver- und entschlüsseln, egal welche Hard- und Software sie gerade verwenden, stehen bisher nicht zur Verfügung.

DE-MAIL MIT ANLAUFSCHWIERIGKEITEN

Mit De-Mail, einer Lösung von verschiedenen großen E-Mail-Providern (u. a. Telekom, GMX, Web.de), die gesetzliche Vorgaben zur rechtssicheren und vertraulichen elektronischen Kommunikation berücksichtigt, gibt es jetzt zwar eine Verschlüsselungslösung, die diese Probleme angeht und eine recht einfache Nutzung ermöglicht, leider ist beim De-Mail-Konzept direkt keine Ende-zu-Ende-Verschlüsselung integriert. Hier werden E-Mails auf den Servern der Provider entschlüsselt und nach Spam oder Schadsoftware untersucht. Eine echte Ende-zu-Ende-Verschlüsselung kann bei De-Mail auch nur durch zusätzliche Techniken wie S/MIME oder PGP erreicht werden, was von vielen Kritikern beanstandet wird. Im Frühjahr 2015 wurde dafür immerhin ein Plug-in vorgestellt, das mit PGP arbeitet. Das Interesse an De-Mail ist bislang weit hinter den Erwartungen zurückgeblieben. Anfang 2015 hat erst knapp eine Million Bundesbürger eine De-Mail-Adresse beantragt. Mehr zur Praxis der E-Mail-Verschlüsselung erfahren Sie in Kapitel 9, in dem es um Verschlüsselungslösungen für verschiedene Kommunikationsformen (Chat, VoIP und E-Mail) geht.

4 SICHERHEIT BEIM ONLINEBANKING

Onlinebanking ist eines der Hauptangriffsziele von Internetkriminellen. Dennoch setzen Geldinstitute immer mehr auf Onlinekontoführung, und auch bei den Kunden kommt das Onlinebanking gut an, bietet es doch einigen Komfort und sorgt für mehr Unabhängigkeit, weil man nicht mehr an Öffnungszeiten gebunden ist. Im Hinblick auf die Sicherheit gleicht die Situation beim Onlinebanking dem Wettrüsten. Auf der einen Seite verbessern Geldinstitute ihre Sicherheitsmaßnahmen immer weiter, auf der anderen Seite ziehen die Kriminellen nach und passen ihre Angriffswerkzeuge und Techniken schnellstens an.

Sicherheitsmaßnahmen

Die klassische Sicherheitstechnik beim Onlinebanking besteht in einer gedruckten TAN-Liste, aus der ein Kunde zusätzlich zur Identifikation per PIN zur Bestätigung einer Transaktion eine beliebige Nummer als Unterschriftersatz eingeben muss. Jede Transaktionsnummer ist nur einmal anwendbar. Die ersten Attacken auf das Onlinebanking waren Phishing-Angriffe, bei denen Kunden unter einem Vorwand dazu gebracht wurden, einige TANs in ein Formular einzutragen, das insgeheim an die Betrüger geschickt wurde, die bereits die PIN ausspioniert hatten.

NR.	TAN	NR.	TAN	NR.	TAN
1	910366	28	146415	55	701679
2	699159	29	188801	56	167247
3	262281	30	912937	57	701540
4	879124	31	704888	58	560861
5	129755	32	836584	59	521067
6	274366	33	227713	60	943142
7	105419	34	265901	61	740322
8	734843	35	141895	62	550596

iTAN-Listen werden immer noch genutzt, neuere Verfahren bieten jedoch mehr Schutz.

Als Gegenreaktion wurden daraufhin indizierte TAN-Listen eingeführt (kurz iTANs), bei denen für eine Transaktion nur noch eine ganz bestimmte der durchnummerierten TANs gültig war. Nutzer konnten sich keine beliebige TAN mehr aussuchen, sondern mussten eine ganz bestimmte TAN-Nummer verwenden. Onlinekriminellen gelang es jedoch immer noch recht häufig, sich in den Besitz gültiger TANs zu bringen, indem sie etwa Nutzer aufforderten, gleich mehrere iTANs in ein Formular einzutragen.

TAN-LISTEN SICHER AUFBEWAHREN

Falls Sie beim Onlinebanking noch mit gedruckten TAN-Listen arbeiten, müssen Sie diese unbedingt sicher aufbewahren. Auf keinen Fall sollten Sie auf diesen Listen die PIN für das Onlinebanking notieren. Gelangen beide Informationen in die Hände von Dritten, ist Ihr Konto in allerhöchster Gefahr. Die PIN für das Onlinebanking sollten Sie möglichst nicht aufschreiben, sondern sich merken. Dies ist recht einfach, da die PIN nicht so komplex und lang ist wie ein konventionelles Passwort. Beim Onlinebanking wird der Zugang bereits nach drei fehlerhaften Eingaben gesperrt, sodass Angreifer durch simples Ausprobieren so gut wie keine Chance haben, selbst wenn nur eine vier- oder fünfstellige PIN genutzt wird.

Obwohl sich auch das iTAN-Verfahren als anfällig erwiesen hat, nutzen immer noch viele Banken und Sparkassen diese Technik. Immer mehr Institute bieten zusätzlich auch andere Verfahren an, die nicht mehr auf gedruckten TAN-Listen basieren, sondern bei denen TANs entweder auf elektronischem Weg übermittelt werden oder der Kunde sie mittels einer zusätzlichen Hardware selbst erzeugt.

Recht verbreitet ist mTAN. Die Abkürzung steht für *mobile TAN*, manchmal wird das Verfahren auch SMS-TAN genannt. Die TAN wird dem Kunden bei Bedarf per SMS auf sein Handy gesendet. Diese TAN ist nur für eine kurze Zeit und die jeweilige Transaktion gültig, außerdem werden die Transaktionsdaten (Betrag, Kontonummer des Empfängers) in der SMS mit angezeigt, um Manipulationen auszuschließen. Diese Daten sollten Sie genau kontrollieren, bevor Sie einen Auftrag mit der TAN freigeben.

Das mTAN-Verfahren erfreut sich großer Beliebtheit, birgt aber auch Risiken. (Foto: Postbank)

GEFAHREN BEI MTAN

Viele Banken und Sparkassen unterstützen mTAN, und viele Kunden nutzen es. Allerdings ist es gerade die Popularität, die Kriminelle lockt. Bei einem Angriff wird nicht nur der PC des Opfers mit einem Trojaner infiziert, sondern auch auf sein Smartphone eine Schadsoftware geschmuggelt. Dadurch können beide Kanäle manipuliert, Daten abgefangen und Transaktionen manipuliert werden. Betroffen sind vor allem Android-Smartphones, andere Mobilplattformen sind besser geschützt. Auf einem Android-Smartphone sollten Sie daher unbedingt eine Antiviren-App installieren, wenn Sie Onlinebanking per mTAN nutzen.

Es gab auch Angriffe, bei denen sich Kriminelle eine zweite SIM-Karte beschafften und darüber an die TANs gelangten, die ja per SMS verschickt wurden. Möglich war dies aufgrund von Sicherheitsdefiziten bei Beantragung und Versand von SIM-Karten bei einigen Mobilfunkprovidern, die mittlerweile angeblich nicht mehr vorhanden sind.

Dadurch, dass die TAN auf einem zweiten, unabhängigen Kommunikationskanal, dem Mobilfunknetz, übertragen wird, sollte dieses Verfahren eigentlich besonders sicher sein. Die mTAN ist ja auch eine Form der Zwei-Faktor-Authentifizierung, denn zusätzlich zum Rechner, an dem das Onlinebanking durchgeführt wird und über den man sich mit der PIN legitimiert, wird hier als zweiter Faktor das Handy bzw. Smartphone verwendet. Angreifer müssen also nicht nur über die Zugangsdaten für das Onlinebanking verfügen, sondern benötigen zusätzlich Zugriff auf das Mobiltelefon, um die TAN in Erfahrung zu bringen.

Die pushTAN-Technik funktioniert ähnlich wie mTAN, allerdings wird die TAN nicht per SMS übermittelt, sondern über eine verschlüsselte Internetverbindung auf ein Smartphone oder Tablet, auf dem eine entsprechende App installiert sein muss. Die TAN ist ausschließlich für den jeweiligen Auftrag gültig, auch werden in der App zusammen mit der TAN ebenfalls noch einmal die Transaktionsdaten angezeigt, die wiederum überprüft werden müssen. Die pushTAN-App ist per Passwort geschützt, und es ist eine Registrierung möglich. Anders als mTAN kann diese Lösung, die vor allem von Sparkassen angeboten wird, auf einfachen Handys nicht zum Einsatz kommen.

Die Nutzung von HBCI-Lesegeräten (das Kürzel HBCI steht für *Home Banking Computer Interface*) gilt schon seit vielen Jahren als sehr sicheres Verfahren, zumindest bei Nutzung hochwertiger Kartenlesegeräte mit einer eigenen Tastatur, die an den Rechner angeschlossen werden müssen. Allerdings waren diese Geräte vergleichsweise teuer (ab ca. 60 Euro) und unhandlich, was die Akzeptanz nicht gerade förderte. Das recht betagte HBCI-Verfahren hat sich daher bis heute nicht durchsetzen können. Mittlerweile gibt es ähnliche Verfahren, die einfacher und flexibler sind und die gleiche oder sogar mehr Sicherheit bieten.

Zu diesen Alternativen gehört das ChipTAN-Verfahren, das als sehr sicher eingestuft wird, sofern Nutzer bei den Transaktionen sorgsam vorgehen. Für dieses Verfahren wird lediglich ein kleines, batteriebetriebenes Lesegerät für die Bankkarte benötigt, das nur wenig größer als die Karte selbst ist. Dieses Gerät ist mittels des Chips in der Karte in der Lage, TANs zu generieren, und zeigt die Transaktionsdaten (Empfänger und Betrag) zur Kontrolle vor der Bestätigung an.

Die Eingabe der Transaktionsdaten in das Gerät kann entweder manuell erfolgen, was etwas mühsam ist, oder über einen Flicker-Code auf der Bank-Webseite. Da das Gerät nicht von Schadprogrammen manipuliert werden kann, ist

dieses Verfahren viel sicherer als mTAN. Ein weiterer Vorteil von ChipTAN ist, dass das Lesegerät nicht nur kompakt, sondern auch vergleichsweise günstig ist (ca. 10 Euro).

ChipTAN gilt als sicher, ist relativ flexibel, und das Lesegerät ist günstig. (Foto: Postbank)

Ähnlich wie der Flicker-Code bei ChipTAN arbeitet auch die photoTAN, bei der mit dem Smartphone eine farbige Grafik auf der Bank-Webseite abfotografiert wird. Mit der photoTAN-App können daraus die Überweisungsdaten ausgelesen und angezeigt werden, anschließend wird eine TAN generiert, die nur für diesen Auftrag gültig ist.

Ganz ohne TAN kommt das BestSign-Verfahren aus, das bei der Postbank angeboten wird. Hierzu benötigen Sie einen USB-Verschlüsselungsstick, den Sie an den Computer anschließen, von dem aus Sie das Onlinebanking nutzen. Der Stick läuft unter Windows, Mac OS und sogar unter einigen Linux-Versionen, für Tablets und Smartphones ist diese Lösung dagegen nicht verfügbar.

Der Bankserver sendet bei dieser Lösung die Transaktionsdaten verschlüsselt an den USB-Stick, der sie entschlüsselt und auf dem kleinen integrierten Display anzeigt. Sie müssen nach der Kontrolle zur Bestätigung des Auftrags

eine Taste auf dem Stick drücken, und schon werden die Auftragsdaten zurückgesendet und ausgeführt. Mit ca. 30 Euro sind die Kosten für den Stick überschaubar. Das System eignet sich auch für Bankkunden, die sehr viele Transaktionen durchführen.

Nicht alle Banken und Sparkassen unterstützen alle diese TAN-Verfahren und Sicherheitstechniken, meist haben Sie nur die Auswahl zwischen zwei oder drei Methoden.

Die folgende Tabelle fasst noch einmal die Eigenschaften der Sicherheitsverfahren zusammen.

SICHERHEITS-VERFAHREN	SICHERHEITSNIVEAU, BESONDERHEITEN	ANBIETER
Einfache TAN-Liste	Unsicher im Hinblick auf Phishing, keine Kontrolle der Transaktionsdaten.	Nur noch Auslaufmodell bei wenigen Instituten.
iTAN	Unsicher im Hinblick auf Phishing, keine Kontrolle der Transaktionsdaten.	Noch bei vielen Instituten, zum Teil schon als Auslaufmodell.
mTAN	Höhere Sicherheit, Rückmeldung der Transaktionsdaten, erhöhtes Risiko auf Android-Smartphones.	Nahezu bei allen Banken und Sparkassen nutzbar, zum Teil wird SMS-Gebühr in Rechnung gestellt.
HBCI-Lesegerät	Hohe Sicherheit bei Nutzung von Lesegeräten mit eigener Tastatur, teure Hardware, geringe Flexibilität.	Bei vielen Banken und Sparkassen nutzbar.
ChipTAN	Hohe Sicherheit, Rückmeldung der Transaktionsdaten, günstige Hardware, größere Flexibilität als HBCI.	Viele Sparkassen, Postbank, VR-Banken, DKB.
pushTAN	Setzt Smartphone oder Tablet voraus, etwas sicherer als mTAN.	Bislang nur bei einigen Sparkassen.
photoTAN	Smartphone oder spezielles Lesegerät, Rückmeldung der Transaktionsdaten.	Commerzbank, Deutsche Bank.
BestSign	Arbeitet mit Signatur statt mit TANs, einfache Bedienung per Stick, Rückmeldung der Transaktionsdaten.	Postbank.

Weitere Schutzmaßnahmen

Komplexe Schadprogramme und Angriffsvarianten zielen auf die Kommunikation mit den Onlinebankservern. So wurden Phishing-Attacken beobachtet, bei denen zusätzlich zur Aufforderung, Zugangsdaten wie PIN und TAN erneut einzugeben, Opfer eine manipulierte Webseite mit einer falschen Servicerufnummer zu sehen bekamen. Skeptische Kunden, die sich hinsichtlich der ungewöhnlichen Aufforderung zur Eingabe der Daten bei der Bank informieren wollten, wurden darüber zu den Telefonanschlüssen der Betrüger geleitet, über die ihnen versichert wurde, dass mit dieser Datenabfrage alles in Ordnung sei.

Ein anderer perfider Trick besteht darin, dass Betrüger nach einem erfolgreichen Betrugsmanöver ihren Raubzug tarnen, indem sie die Onlineanzeige der Überweisungen und des Kontostands manipulieren. Dadurch soll verhindert werden, dass der Betrug frühzeitig bemerkt und der überwiesene Betrag noch rechtzeitig zurückgebucht werden kann.

Mit dieser Technik arbeitet auch ein Trick, der völlig unabhängig von der benutzten Sicherheitstechnik funktioniert. Hier blendet die Schadsoftware beim Aufruf der Banking-Website den Hinweis ein, dass das Konto für Transaktionen vorübergehend gesperrt sei, weil auf diesem irrtümlicherweise ein höherer Betrag gutgeschrieben wurde und diese Summe zurücküberweisen werden müsse. Die Freischaltung des Kontos soll sofort nach der Rücküberweisung erfolgen. Die elektronische Umsatzanzeige zeigt zur Bestätigung den entsprechenden Geldeingang und den Kontostand an. Wer der Aufforderung nachkommt und das Geld auf das angegebene Konto überweist, erlebt eine böse Überraschung: Den Geldeingang hatte es nie gegeben, stattdessen ist das eigene Geld weg.

Bei dieser Art des Social Engineering müssen sich die Kriminellen gar nicht um eine TAN bemühen, da das Opfer die Überweisung ja freiwillig selbst ausführt. Bei vielen Angriffen werden die Opfer zuvor überwacht, und die Angriffe folgen erst, wenn das Konto gut gefüllt ist. Bei potenziellen Opfern, die neben dem Girokonto Wertpapierdepots oder Festgeldkonten online führen, gehen Betrüger auch mehrstufig vor. Zunächst überweisen sie Geld vom Festgeldkonto auf das Girokonto oder verkaufen sogar Wertpapiere, erst danach plündern sie das Verrechnungskonto.

Ähnlich arbeiteten Angreifer auch, als sie im Zuge der Umstellung auf das SEPA-Verfahren Opfer aufforderten, eine Testüberweisung von 1 Cent auf das Konto der Bank durchzuführen. Im Webinterface wurde ein entsprechend

ausgefülltes Überweisungsformular eingeblendet. Bei Bestätigung des Auftrags durch eine TAN wurde die Schadsoftware nochmals aktiv und leitete den Auftrag nicht weiter, sondern änderte Überweisungssumme und Empfänger. Nutzer von moderneren TAN-Verfahren wie mTAN oder ChipTAN wäre diese Manipulation durch die Rückmeldung der Transaktionsdaten vielleicht aufgefallen, bei den alten TAN- bzw. iTAN-Methoden blieb sie dagegen unbemerkt.

RICHTEN SIE EIN LIMIT FÜR DAS ONLINEBANKING EIN

Bei den meisten Onlinebanken haben Sie die Möglichkeit, eine Höchstgrenze für Onlinetransaktionen festzulegen. Damit können Sie zumindest die Schadenshöhe begrenzen. Eine Änderung des Limits sollte dann aber nicht mehr online möglich sein. Haben Angreifer die Kontrolle über Ihren Rechner, könnten sie sonst die Änderung des Limits selbst in Auftrag geben und anschließend das Konto leer räumen.

Noch vorsichtiger sein

Wenn Sie mit Ihrem Computer Onlinebanking nutzen, müssen Sie besonders vorsichtig sein. Alle Schutzmaßnahmen im Hinblick auf das Surfen im Web, die Absicherung des Systems durch Softwareaktualisierungen und die Phishing-Vorsichtsmaßnahmen sollten Sie unbedingt beachten. Auch sollten Sie vorsichtig bei der Installation von Software sein und die Browsersicherheitseinstellungen erhöhen.

Rufen Sie die Webseiten für Onlinebanking immer nur durch direkte Eingabe der Adresse auf oder über einen Eintrag im Favoritenordner. Wenn Ihnen ein Link zur Banking-Seite per E-Mail zugesandt wird, sollten Sie sehr skeptisch sein, da Sie darüber auf eine gefälschte Website umgeleitet werden könnten. Eine weitere Betrugsvariante ist nämlich das sogenannte Pharming. Dabei wird die Namensauflösung, bei der die konventionelle Internetadresse (URL), die Sie in den Browser eingeben, in die numerische IP-Adresse des Servers umgewandelt wird, so manipuliert, dass Sie nicht auf dem echten Bankserver landen, sondern auf dem Server der Betrüger mit den gefälschten Webseiten.

Umso wichtiger ist es daher, dass Sie beim Aufruf Ihrer Onlinebanking-Website nicht nur auf die Sicherheit der Übertragung achten, sondern sich wie im vorigen Kapitel beschrieben auch die Zertifikate ansehen, mit denen die Identität der Website bestätigt wird.

Höchste Sicherheit durch Live-Systeme

Wollen oder benötigen Sie höchste Sicherheit für Ihre Bankgeschäfte, können Sie ein Live-System einsetzen. Dabei verwenden Sie Ihren Rechner nicht in der üblichen Form über das installierte Betriebssystem, sondern starten den PC über eine CD/DVD oder einen USB-Stick, auf dem ein alternatives Betriebssystem genutzt wird. Selbst wenn auf der Festplatte Ihres Rechners ein unerkannter Trojaner vorhanden ist, kann dieser beim Onlinebanking keinen Schaden anrichten, da die Festplatte gar nicht genutzt wird.

Derartige Live-CDs bieten verschiedene Computermagazine regelmäßig an. Normalerweise handelt es sich bei den Live-Systemen um angepasste Linux-Varianten, die auch auf jedem Windows-PC laufen. Auf dem System sind alle Treiber und Programme vorhanden, um direkt eine Internetverbindung herzustellen und Webseiten sowie das Onlinebanking zu nutzen. Live-Systeme können durch Schadsoftware-Angriffe nicht manipuliert werden, da auf den Datenträgern keine Änderungen möglich sind.

Legen Sie die CD oder DVD in das Laufwerk ein, wird beim Hochfahren das Live-System automatisch gestartet. Ist das nicht der Fall, müssen Sie die Startreihenfolge im Bootmenü anpassen. Hat Ihr Rechner kein optisches Laufwerk, können Sie das Live-System auf einem USB-Stick installieren, den Sie anstelle


PC-WELT Banking-DVD

Montag den 11.08.2014 um 12:30 Uhr

von Simon Pfaab

Direkt zum Download

PC-WELT Banking-DVD

Update:	23.06.2014
Downloads:	1270
Softwareart:	GNU
Sprache:	Deutsch
System(e):	Windows XP, Windows Vista, Windows 7, Windows 8

Damit Kriminelle nicht mit fiesen Tricks auf Ihre Online-Banking-Daten zugreifen, schützen Sie sich vor den Gefahren mit dem Live-System PC-WELT Banking DVD.

Fast alle Angriffe auf Online-Banking-Nutzer setzen voraus, dass die Kriminellen einen Virus auf dem PC des Opfers installieren. Damit Ihnen das nicht passiert, können Sie ein auf Linux basierendes Live-System nutzen und damit fürs Online-Banking den PC starten. Live-System bedeutet, dass das Betriebssystem nicht auf dem PC installiert wird, sondern als bereits lauffähiges und unveränderbares System startet. Wird das System beendet, speichert es keine Veränderungen, wodurch ein Virenangriff nur extrem schwer möglich ist.

Ein solches Live-System erhalten Sie kostenlos als

Verschiedene Computermagazine wie die PC-Welt bieten Live-CDs zum sicheren Onlinebanking an.

einer CD/DVD nutzen. Meist haben Sie die Möglichkeit zum Download einer ISO-Datei, die Sie auf einen USB-Stick kopieren können.

Live-Systeme gibt es von Magazinen wie Computerbild, PC-Welt oder der c´t. Die wohl bekannteste Lösung ist c´t-Knoppix, das auch eine Finanzverwaltungssoftware mitbringt, die Sie optional für Ihre Onlinebankgeschäfte verwenden können.

Die meisten Angriffe beim Onlinebanking zielen auf die Nutzung der Webangebote, und die Schadprogramme sind vor allem auf Windows-PCs spezialisiert. Sie können das Risiko daher schon allein dadurch reduzieren, dass Sie auf ein anderes Betriebssystem ausweichen, wie es ja bei den eben beschriebenen Live-CDs der Fall ist. Ebenso können Sie zum Onlinebanking spezielle Banking-Software verwenden und nicht mehr den konventionellen Weg via Browser und Website der Bank gehen.

BANKING-PROGRAMME STATT WEBBANKING

Mit Anwendungen wie Quicken oder Star Money, um nur zwei der bekanntesten Tools zu nennen, können Sie nicht nur komfortabel mehrere Konten verwalten, diese Programme bieten auch zahlreiche Extras. Dadurch, dass Sie Überweisungen und andere Zahlungsvorgänge nicht direkt auf der Webseite der Bank vornehmen, sondern sie auch offline erledigen können, sind Sie recht sicher. Spezielle Attacken auf Banking-Programme sind bislang jedenfalls nicht bekannt.

Ausweichen können Sie auch auf Apps für Tablets und Smartphones, die viele Banken und Sparkassen für das Onlinebanking anbieten. Auch hier sind bislang kaum Attacken bekannt geworden, allerdings könnte sich diese Situation schnell ändern.

So wurde etwa Anfang 2015 eine Sicherheitslücke (UXSS) entdeckt, von der alle älteren Android-Versionen bis einschließlich Version 4.3 betroffen sind. Über dieses Leck, das sich in den Android-Browsern befindet, können Daten ausspioniert werden, sodass unbedingt andere Browser-Apps eingesetzt werden sollten. Auch Apps, die zur Anzeige von Webinhalten auf den Android-Webbrowser zugreifen, sind durch die Lücke verwundbar.

Wenn Sie eine Smartphone-App für das Onlinebanking nutzen, dürfen Sie sich auf keinen Fall beim mTAN-Verfahren die Transaktionsnummern ebenfalls auf dieses Gerät senden lassen. Die Zwei-Faktor-Lösung, die die eigentliche Stärke

dieses Systems ist, wird damit ausgehebelt. Wenn Dritte Zugang zum Gerät bekommen, ist die Gefahr, dass sie damit auch Verfügungsgewalt über das Konto bekommen, viel zu groß. Die meisten Geldinstitute, die App-Lösungen anbieten, schließen dies in den Geschäftsbedingungen daher auch explizit aus.

HAFTUNGSFRAGEN

Wenn es zu einem Schaden beim Onlinebanking kommt, haben Sie gute Chancen, dass Ihnen Ihre Bank die entwendete Summe erstattet. Keinen Erstattungsanspruch gibt es allerdings, wenn Sie den Schaden selbst durch grobe Fahrlässigkeit oder Vorsatz verschuldet haben. Dies trifft schon dann zu, wenn Sie auf Ihrem PC keine aktuelle Antivirensoftware verwenden oder sich die PIN notieren und zusammen mit der TAN-Liste aufbewahren. Außerdem sollten Sie die Sicherheitshinweise der Institute zum Onlinebanking befolgen, um Schwierigkeiten vorzubeugen. Ist ein Schaden eingetreten, müssen Sie unverzüglich Ihre Bank informieren und eine Erstattung fordern. Außerdem müssen Sie Strafanzeige erstatten, zur Beweissicherung Ihren PC mit einer Antivirensoftware überprüfen und diesen Bericht ausdrucken.

Hundertprozentige Sicherheit wird es beim Onlinebanking niemals geben. Gleiches gilt aber auch für die konventionelle Kontoführung, bei der es ja ebenfalls Risiken gibt. Wenn Sie die grundlegenden Sicherheitsregeln beachten und noch etwas vorsichtiger und aufmerksamer als beim normalen Surfen sind, gibt die Gefahrenlage beim Onlinebanking keinen besonderen Grund zur Besorgnis.

Die wichtigsten Sicherheitsmaßnahmen und Tipps haben wir für Sie in der folgenden Auflistung noch einmal zusammengefasst:

- Verwenden Sie auf Ihrem PC eine aktuelle Antivirensoftware, um vor Angriffen durch Schadsoftware geschützt zu sein.
- Beachten Sie die Tipps zum sicheren Surfen im Web und zur Phishing-Vorbeugung aus dem letzten Kapitel (Betriebssystem und Software aktualisieren, Browsersicherheitseinstellungen, Phishing-Filter verwenden, Umgang mit verdächtigen E-Mails etc.). Erhöhen Sie gegebenenfalls die Sicherheit in den Einstellungen.
- Reagieren Sie auf keinen Fall auf E-Mails oder unerwartet eingeblendete Fenster während des Onlinebankings, in denen Sie zur Eingabe von PIN und TANs aufgefordert werden. Fragen Sie im Zweifelsfall lieber bei Ihrem Geldinstitut nach. ▸

- Überprüfen Sie die Sicherheit der Verbindung beim Onlinebanking und die Zertifikate der Banking-Websites. Rufen Sie diese Seiten immer direkt per Adresseingabe oder über Ihre Favoritenliste (Lesezeichen) auf.
- Entscheiden Sie sich beim Onlinebanking für ein sicheres TAN-Verfahren. Erkundigen Sie sich, welche Varianten Ihre Bank anbietet.
- Nutzen Sie das mTAN-Verfahren (SMS-TAN) mit einem Android-Smartphone, sollten Sie auf diesem eine Antivirensoftware verwenden und vorsichtig bei der Installation von Software sein.
- Nutzen Sie eine sichere PIN zur Anmeldung beim Onlinebanking und wechseln Sie sie regelmäßig. Verwenden Sie gedruckte TAN-Listen, müssen Sie sie sicher und dürfen sie vor allem niemals zusammen mit der PIN aufbewahren. Die PIN sollten Sie nach Möglichkeit gar nicht notieren. Falls Sie der Meinung sind, dies doch tun zu müssen, sollten Sie die Notiz in jedem Fall an einem sehr sicheren Ort aufbewahren.
- Weichen Sie auf einem Windows-Rechner gegebenenfalls auf die Nutzung einer Live-CD für das Onlinebanking aus. Macs und Linux-Rechner sind deutlich sicherer als Windows-Systeme.
- Verwenden Sie gegebenenfalls eine Banking-Software, um die direkte Nutzung der Webseiten beim Onlinebanking zu umgehen. Auch damit reduzieren Sie das Risiko.
- Nutzen Sie gegebenenfalls Banking-Apps für Mobilplattformen. Momentan sind auch diese Lösungen nicht so gefährdet wie das Onlinebanking per PC und Web. Das geringste Risiko gibt es bei iOS und Windows Phone, bei Android ist die Bedrohung dagegen größer und der Einsatz einer Antivirensoftware daher unumgänglich.
- Vereinbaren Sie mit dem Geldinstitut ein Limit für das Onlinebanking, sofern dies praktikabel ist. Kontrollieren Sie die Umsätze beim Onlinebanking in möglichst kurzen Abständen.
- Nutzen Sie nach Möglichkeit keine öffentlichen Rechner (z. B. Internetcafé, Bibliothek etc.) für das Onlinebanking. Falls es doch einmal notwendig ist, sollten Sie nach dem Ausloggen den Browsercache löschen.
- Fallen Ihnen während des Onlinebankings Merkwürdigkeiten auf, werden Sie etwa aufgrund von Verbindungsproblemen oder mit anderen Begründungen zur erneuten Eingabe von PIN oder TAN aufgefordert, brechen Sie die Transaktion ab und wenden sich am besten telefonisch an die Bank.
- Haben Sie eine Manipulation festgestellt und wurde Ihr Konto geplündert, benachrichtigen Sie unverzüglich Ihr Geldinstitut. Wird eine illegale Abbuchung direkt entdeckt, kann sie mit etwas Glück noch rückgängig gemacht werden.

5 SICHERES ONLINESHOPPING

Einkaufen im Web ist zu einer Selbstverständlichkeit geworden. Längst sind es nicht mehr nur Bücher, Musik oder Elektronikartikel, die online erworben werden, die meisten Surfer bestellen auch zahlreiche andere Güter des alltäglichen Bedarfs oder geben via Internet Dienstleistungen in Auftrag. Anders als im realen Leben gibt es hier allerdings keinen persönlichen Kontakt zwischen Käufer und Verkäufer, und auch eine eindrucksvolle Website und großartige Werbeversprechen sind nicht zwangsläufig ein Indiz für Seriosität. Bei Beachtung einiger Grundregeln muss das Einkaufen und Bezahlen im Internet jedoch keineswegs unsicherer sein als im echten Leben.

5.1 Sicher einkaufen

Das Web ist die größte Shopping-Mall der Welt. Bequem können Sie vom PC aus oder per Smartphone bei Tausenden von Onlineshops Waren ordern und bequem zu sich nach Hause liefern lassen. Neben den Großen der Branche, die mit einer riesigen Produktpalette keine Wünsche offen lassen, gibt es zahlreiche kleine Shops, die dafür mit einem exklusiven oder spezialisierten Angebot punkten.

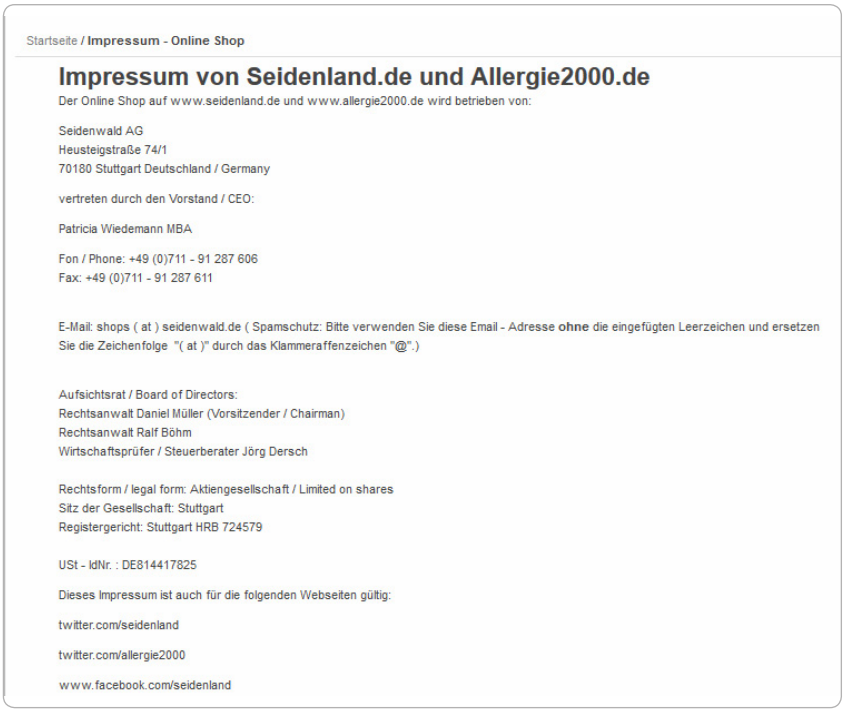
Beim Einkaufen im Web ist eine Registrierung notwendig. Spätestens wenn Sie in einem Shop das erste Mal an die virtuelle Kasse gehen, müssen Sie sich anmelden und Ihre Daten angeben. Neben Angaben wie Name, Alter, Anschrift und E-Mail-Adresse betrifft dies auch finanzielle Informationen wie Kreditkartennummer oder Kontoverbindung, je nach gewähltem Zahlungsverfahren.

Onlineshop überprüfen

Ihre Daten sind in diesem Zusammenhang als besonders schützenswert zu betrachten und sollten ausschließlich an vertrauenswürdige Geschäftspartner übermittelt werden. Bevor Sie das erste Mal in einem Onlineshop einkaufen, sollten Sie sich den Anbieter etwas genauer ansehen. Bei den Großen der Branche können Sie sicher den einen oder anderen Aspekt weglassen, denn die prinzipielle Seriosität dieser Anbieter ist ja bereits durch Millionen von erfolgreichen Transaktionen bestätigt.

Die Überprüfung können Sie direkt auf der Website des Onlineshops beginnen. Hier sollte schnell und direkt die Anbieterkennung (Webimpressum) zu finden sein. Sie muss unter anderem folgende Angaben enthalten:

- Name und Anschrift, bei juristischen Personen die Rechtsform. Ein Postfach als Anschrift ist nicht ausreichend.
- Informationen, die eine schnelle Kontaktaufnahme ermöglichen, wie etwa Telefonnummer, Faxnummer, E-Mail-Adresse.
- Angaben zu Handelsregister, gegebenenfalls Gewerberegister und Gewerberegisternummer.
- Umsatzsteueridentifikationsnummer.
- Bei bestimmten Anbietern, die spezielle Zulassungen (beispielsweise Apotheken) voraussetzen, Angaben zu den Aufsichtsbehörden und gegebenenfalls zu den Kammern, in denen sie Mitglied sind.



Startseite / **Impressum - Online Shop**

Impressum von Seidenland.de und Allergie2000.de

Der Online Shop auf www.seidenland.de und www.allergie2000.de wird betrieben von:

Seidenwald AG
Heusteigstraße 74/1
70180 Stuttgart Deutschland / Germany

vertreten durch den Vorstand / CEO:

Patricia Wiedemann MBA

Fon / Phone: +49 (0)711 - 91 287 606
Fax: +49 (0)711 - 91 287 611

E-Mail: shops (at) seidenwald.de (Spamschutz: Bitte verwenden Sie diese Email - Adresse **ohne** die eingefügten Leerzeichen und ersetzen Sie die Zeichenfolge "(at)" durch das Klammeraffenzeichen "@".)

Aufsichtsrat / Board of Directors:
Rechtsanwalt Daniel Müller (Vorsitzender / Chairman)
Rechtsanwalt Ralf Böhm
Wirtschaftsprüfer / Steuerberater Jörg Dersch

Rechtsform / legal form: Aktiengesellschaft / Limited on shares
Sitz der Gesellschaft: Stuttgart
Registergericht: Stuttgart HRB 724579

USt - IdNr. : DE814417825

Dieses Impressum ist auch für die folgenden Webseiten gültig:

twitter.com/seidenland

twitter.com/allergie2000

www.facebook.com/seidenland

Das Impressum eines Onlineshops muss unter anderem eine Kontaktadresse enthalten.

Neben dem Impressum sollten Sie sich auch die allgemeinen Geschäftsbedingungen (AGB) anschauen, die ebenfalls leicht erreichbar auf der Website abrufbar sein müssen. Außerdem sind für Onlineshops folgende Angaben vorgeschrieben, und es ist in jedem Fall ratsam, sich diese vor dem Kauf anzusehen:

- Informationen zu Datenschutz und Datensicherheit.
- Informationen zu Widerrufsrecht, Rückgaberecht und Erstattung des Kaufpreises.
- Angaben zu Versand- und Rücksendekosten.
- Übersicht der angebotenen Zahlungsmethoden.

Sind diese Daten vorhanden und entsprechen auch inhaltlich den Anforderungen, können Sie vor einer Bestellung zusätzliche Webrecherchen unternehmen, um Meinungen von Kunden einzuholen, die bereits in diesem Shop eingekauft haben. Hier bieten sich Portale wie Shopauskunft (*www.shopauskunft.de*) oder Shopvote (*www.shopvote.de*) an, aber auch auf allgemeinen Bewertungsportalen und Preisvergleichsdiensten werden Sie fündig. Bei kleineren Shops kann es hilfreich sein, den Namen zusammen mit Begriffen wie »Bewertung« oder »Problem« in eine der großen Suchmaschinen einzugeben.

Die Bewertungen der Shops durch andere Nutzer können eine Hilfe sein.

HINTERFRAGEN SIE BEWERTUNGEN

Die Beurteilung eines Shops (oder auch von Produkten oder Dienstleistungen) durch andere Käufer kann für mehr Transparenz sorgen, es gibt aber auch bedenkliche Entwicklungen. So werden Beurteilungen auf Verbraucherportalen oder Vergleichsseiten manipuliert, indem im Auftrag des Anbieters Agenturen positive Kommentare und Meinungen verfassen. Umgekehrt gibt es auch negative Beurteilungen, die von Konkurrenten in Auftrag gegeben werden, die das Gesamturteil massiv beeinflussen. Vor allem in Hotelbewertungsportalen sind diese Manipulationen verbreitet. Sie sollten daher immer skeptisch bleiben.

Gütesiegel für Shops

Ein Qualitätsindikator können Gütesiegel unabhängiger Einrichtungen sein, die an Shops vergeben werden, wenn sie bestimmte Anforderungen erfüllen. Es gibt eine Vielzahl derartiger Gütesiegel, allerdings stammen nicht alle von wirklich unabhängigen und neutralen Organisationen. Manchmal haben auch anbieternahe Institutionen Siegel entwickelt, die niedrigere Standards voraussetzen und nur eine geringe Aussagekraft haben.

Aber auch zwischen renommierten Gütesiegeln gibt es größere Unterschiede. Die Anforderungskataloge und Prüfkriterien, die die Shops erfüllen müssen, weichen stark voneinander ab. Bei einigen stehen Eigenschaften wie Kundenservice, Transparenz und Bedienbarkeit der Shopsysteme im Mittelpunkt, andere achten besonders auf Aspekte wie Datenschutz und Datensicherheit.

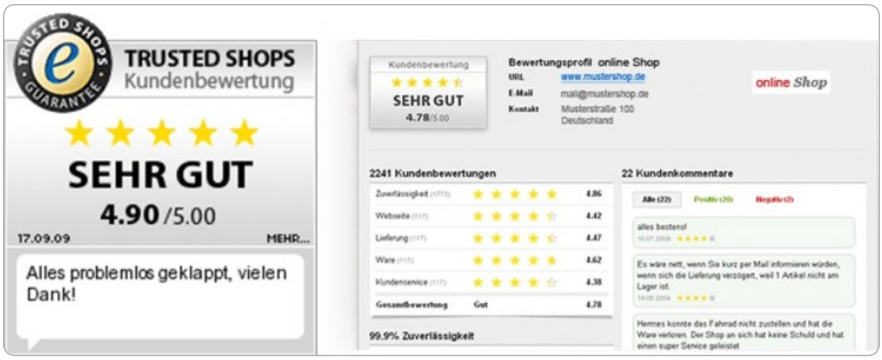
KUNDENSCHUTZ BIETET SICHERHEIT

Bei einigen Gütesiegeln ist ein Käuferschutz enthalten. Dieser Käuferschutz bietet Kunden zusätzliche Sicherheit, sollte es zu Problemen kommen. So gibt es z. B. eine Versicherung, wenn Ware nach der Bezahlung nicht geliefert wird oder der Verkäufer nach Wahrnehmung des Widerrufsrechts und Rücksendung der Ware den Kaufpreis nicht erstattet.

Zu den allgemein anerkannten und respektierten Gütesiegeln gehören folgende Programme:

- Trusted Shops
- S@fer Shopping (TÜV Süd)
- Geprüfter Online Shop (EHI)
- Internet Privacy Standards (ips)

Trusted Shops ist das bekannteste Qualitätssiegel für Onlineshops, und europaweit haben sich bereits knapp 20.000 Shops zertifizieren lassen. Das System beinhaltet einen Käuferschutz, der für alle Käufe bis zu einem Betrag von 2.500 Euro kostenlos ist. Optional können gegen Aufpreis auch höhere Kaufbeträge abgesichert werden. Trusted Shops bietet dazu ein eigenständiges Bewertungssystem für die teilnehmenden Onlineshops an.



Trusted Shops ist das bekannteste Gütesiegel auf dem Markt.

Das vom TÜV Süd angebotene S@fer Shopping konzentriert sich bei der Zertifizierung vorrangig auf die von den Onlineshops genutzte Technik und beurteilt deren Zuverlässigkeit und Sicherheit, die letztlich auch für die Datensicherheit verantwortlich ist. Die Prüfung durch den TÜV Süd erfolgt auch vor Ort bei den Anbietern.

S@fer Shopping des TÜV Süd wird ebenfalls sehr oft genutzt.

Vom wissenschaftlichen Institut des Handels stammt das weitverbreitete EHI-Gütesiegel, das von unabhängigen Experten als seriös eingestuft wird. Nach Angaben des Instituts nutzt fast jeder zweite der umsatzstärksten Shops dieses Siegel. Verbraucher können sich bei Beschwerden, die nicht einvernehmlich mit dem Shopbetreiber geklärt werden, über ein Onlinebeschwerdeformular direkt an das Institut wenden, das wiederum in Kontakt mit dem Onlineshop tritt.

Das EHI-Gütesiegel ist ebenfalls sehr verbreitet.

Ein weiteres renommiertes Siegel ist Internet Privacy Standards, das von der Datenschutz Cert GmbH vergeben wird. Bei diesem Siegel werden allerdings primär die Bereiche Datenschutz und Sicherheit sowie die Sicherheit der Datenspeicherung und Datenübertragung überprüft, während andere Aspekte nicht oder nur am Rande berücksichtigt werden.

Beim IPS-Siegel werden vorrangig Aspekte der Datensicherheit geprüft.

Besonderheiten beim Kauf in ausländischen Webshops

Das Web eröffnet beim Onlineshopping neue Welten, da auch Anbieter aus fremden Ländern nur einen Mausklick entfernt sind. Beim grenzüberschreitenden Einkauf sollten Sie allerdings einige zusätzliche Dinge beachten, damit Sie nach dem Kauf nicht doch eine böse Überraschung erleben.

Beim Einkauf im Ausland können Sie sich nicht immer auf das vergleichsweise verbraucherfreundliche deutsche Recht verlassen. Normalerweise gilt innerhalb der EU die Regel, dass bei Streitigkeiten das Recht des Landes gilt, in dem der Verkäufer ansässig ist. Es gibt aber auch Ausnahmen, etwa wenn der Unternehmer den Shop so ausgerichtet hat, dass er eindeutig auf Käufer in anderen Staaten zielt. In so einem Fall, wenn also der ausländische Shop spezielle deutschsprachige Seiten bietet, deutsche Kunden anspricht und die Lieferung nach Deutschland zusagt, könnten auch die deutschen Verbraucherschutzregeln gelten. Es dürfte allerdings im Zweifelsfall schwer sein, sie durchzusetzen. Hinzu kommt, dass der Aufwand oft in keinem Verhältnis zum möglichen Schaden steht, sodass im Zweifelsfall eine juristische Auseinandersetzung eher nicht infrage kommt.

Beim Kauf im Ausland sollten Sie besonders auf die Versandkosten achten. Diese sind häufig deutlich höher als die Kosten für einen konventionellen Versand im Inland. Manchmal kann sich durch die hohen Versandkosten ein möglicher Preisvorteil bei der Bestellung im Ausland ins Gegenteil verkehren.

KAUFEN IM AUSLAND KANN TEUER WERDEN

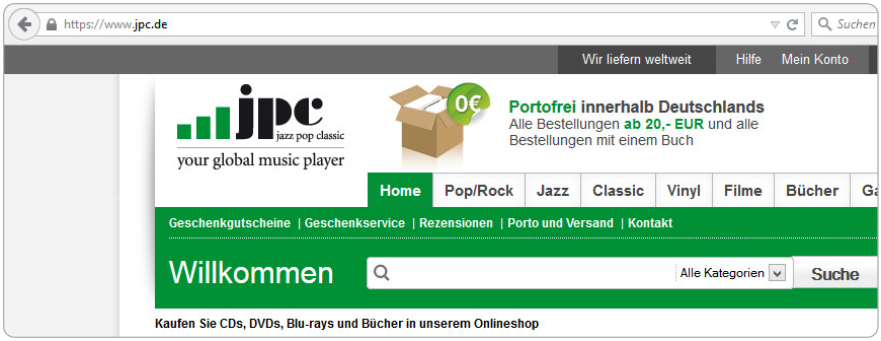
Deutlich teurer als gedacht kann das Einkaufen in ausländischen Shops außerhalb der EU durch zusätzliche Einfuhrabgaben werden. Hierzu zählen neben Zöllen auch Einfuhrumsatzsteuern und Verbrauchssteuern für bestimmte Güter (wie etwa Tabaksteuer oder Branntweinsteuer). Die Einfuhrumsatzsteuer entspricht der deutschen Mehrwertsteuer und wird auf Warensendungen im Wert von über 22 Euro erhoben. Für Zölle gilt eine Grenze von 150 Euro. Bei Verbrauchssteuern kann es auch bei Warensendungen aus dem EU-Ausland zu Aufschlägen kommen, wovon etwa Spirituosen oder Zigaretten betroffen sind. Gute Shops informieren über diese zusätzlichen Belastungen vor dem Kauf.

Ärger mit dem Zoll kann es auch geben, wenn Waren importiert werden, die in Deutschland nicht zugelassen sind, weil sie gesetzlichen oder technischen Anforderungen nicht genügen. Gefälschte Markenprodukte oder Plagiate, wie sie manchmal bei eBay von ausländischen Händlern angeboten werden, werden ebenfalls immer wieder bei der Einfuhr beschlagnahmt.

Verschlüsselte Verbindungen

Für das Onlineshopping gelten ähnliche Regeln wie fürs Onlinebanking. Auch hier übertragen Sie beim Bezahlvorgang schützenswerte Daten, und wenn diese in fremde Hände geraten, kann ein Missbrauch negative Folgen für Sie haben.

In jedem Fall sollten bei der Anmeldung, aber auch beim Bezahlvorgang, Ihre Daten verschlüsselt übertragen werden. Wie immer erkennen Sie dies im Browser am Kürzel *https* in der Adresszeile und am Symbol des geschlossenen Vorhängeschlosses. Die Nutzung dieser Verschlüsselungstechnik ist längst obligatorisch und eine absolute Notwendigkeit, um eines der beschriebenen Gütesiegel zu erlangen.



Die Datenübertragung beim Onlineshopping sollte verschlüsselt erfolgen.

WÄHLEN SIE PASSWÖRTER SORGFÄLTIG

Ihre Konten bei Onlineshops sollten Sie gut absichern, indem Sie ein sicheres Passwort verwenden. Auch wenn Sie nur selten in einem Shop einkaufen und es daher schwer ist, sich ein komplexes, ausreichend langes Passwort aus einer zufälligen Zeichenfolge zu merken, dürfen Sie nicht der Versuchung erliegen, ein zu einfaches Passwort zu wählen.

Widerrufsrecht und Rücksendung

Als Käufer in einem Onlineshop haben Sie die Möglichkeit, den Kaufvertrag ohne Angabe von Gründen zu widerrufen. Im Onlineshop muss es dazu einen entsprechenden Hinweis geben. Die Widerrufsfrist beträgt normalerweise 14 Tage, einige Händler räumen aber auch freiwillig einen längeren Zeitraum ein.

In diesem Zeitraum können Sie die bestellte Ware zurücksenden, und der Verkäufer erstattet im Gegenzug die Kaufsumme. Bei bestimmten Waren (etwa verderblichen Lebensmitteln) ist dieses Widerrufsrecht eingeschränkt, auch beim Kauf digitaler Güter, etwa dem Download von Software, Musik oder Videos, ist ein Ausschluss des Widerrufsrechts möglich. Außerdem kann der Händler einen Wertersatz fordern, wenn der Wert der gelieferten Ware durch Ingebrauchnahme reduziert wurde.

Bis ins Jahr 2014 waren Händler verpflichtet, die Kosten der Rücksendung im Fall eines Widerrufs zu tragen, sofern der Warenwert die Grenze von 40 Euro

überstieg. Diese Vorgabe ist mit dem neuen Widerrufsrecht hinfällig geworden, und die Rücksendungskosten können jetzt unabhängig vom Preis immer dem Käufer auferlegt werden. Allerdings verzichten in Deutschland die meisten großen Onlineshops auf diese Möglichkeit und übernehmen die Kosten nach wie vor freiwillig. Kleinere Anbieter halten ebenfalls häufig noch an dieser Praxis fest.

Sonderfall Auktionen

Auktionen nehmen beim Einkaufen im Web eine Sonderrolle ein. So agieren auf Auktionsplattformen wie eBay neben vielen kleinen Händlern auch zahlreiche Privatanbieter. Während für gewerbliche Anbieter hier weitgehend die gleichen Vorgaben gelten wie beim normalen Onlinehandel, gibt es bei Geschäften zwischen Privatpersonen in vielerlei Hinsicht andere Regeln, etwa im Hinblick auf die Gewährleistungspflichten.

Ohne hier auf die juristischen Details einzugehen, gibt es beim Kauf von privaten Anbietern ein höheres Risiko als beim Erwerb eines Produkts bei einem gewerblichen Verkäufer. Aber auch bei den gewerblichen Anbietern handelt es sich meistens nicht um große und zumeist seriöse Handelsunternehmen, sondern um unbekannte, kleinere Händler.

BEACHTEN SIE DIE BEWERTUNGEN

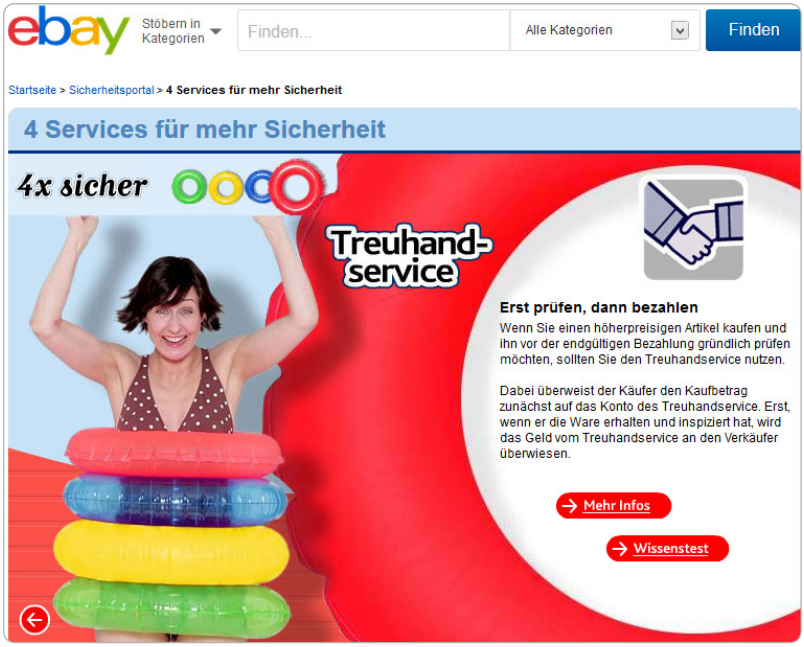
Die wichtigste Informationsquelle zur Beurteilung der Seriosität und Zuverlässigkeit eines Anbieters auf eBay sind die Bewertungen der bisherigen Transaktionen. Sie sollten sich diese genau anschauen und auf verdächtige Veränderungen achten. Hat sich in jüngster Zeit die Zahl der negativen Bewertungen deutlich erhöht, kann das ein ernst zu nehmender Warnhinweis sein. Problematisch kann es auch werden, wenn ein Anbieter viele positive Bewertungen hat, bislang aber nur billige Artikel angeboten hat und nun auf einmal hochpreisige Güter anbietet.

Bei teuren, höherwertigen Gebrauchtwaren sollten Sie im Zweifelsfall Kontakt zum Verkäufer aufnehmen und nach Belegen wie Kaufnachweisen und Ähnlichem fragen. Sofern das möglich und im Hinblick auf den Aufwand vertretbar ist, kann sogar eine Besichtigung vor dem Kauf angeraten sein, bei der Sie sich vor Ort über Zustand und Qualität des Objekts vergewissern können.

VORSICHT BEI VORKASSE

Hinsichtlich der Zahlungsmodalitäten sollten Sie zumindest bei größeren Beträgen auf sichere Verfahren bestehen. Vorkasse, wie sie gerade bei privaten Auktionen immer noch häufig verwendet wird, ist bei höheren Beträgen viel zu unsicher. Das Bezahlen per PayPal bietet einen gewissen Schutz sowohl für Käufer als auch für Verkäufer, allerdings hat auch dieses System seine Grenzen.

Bei besonders hohen Rechnungsbeträgen kann die Nutzung eines Treuhandservice angeraten sein, obwohl das die Kosten erhöht. Bei einem Treuhandservice wird der Betrag zunächst an eine Abwicklungsstelle überwiesen. Diese teilt dem Anbieter den Geldeingang mit, woraufhin der die Ware abschickt. Erst wenn der Käufer die Ware in der verabredeten Qualität erhält und das bestätigt, überweist der Treuhandservice den Kaufpreis an den Verkäufer.



Bei teuren Anschaffungen auf eBay sollten Sie den Treuhandservice nutzen.

Die Barzahlung von höheren Beträgen, etwa beim Kauf eines Gebrauchtwagens, ist oftmals bedenklich. In der Vergangenheit hat es immer wieder Fälle gegeben, bei denen Käufer bei der Übergabe brutal überfallen und ausgeraubt wurden. Sie sollten daher skeptisch sein, wenn der Verkäufer auf dieser Zahlungsmethode besteht.

Skepsis ist auch angeraten, wenn beim Bezahlen eine Diskrepanz zwischen Verkäufer und Empfängerkonto auftritt. Stimmen die Namen nicht überein, sollten Sie nachfragen und sich das erklären lassen. Zahlungen auf ausländische Konten sind ebenfalls verdächtig, wenn der Verkäufer ansonsten über eine deutsche Adresse erreichbar ist. Zahlungen über Dienste wie Western Union sollten Sie ebenfalls nicht vornehmen.

LESEN SIE AUKTIONSANGEBOTE IMMER SEHR GENAU

Bevor Sie auf einen Artikel bieten, sollten Sie sich den Angebotstext immer ganz genau durchlesen. Mitunter finden sich in den Beschreibungen gut versteckt Hinweise auf Beschädigungen, Defekte oder sonstige Einschränkungen. Es hat schon Fälle gegeben, bei denen Produktverpackungen hochwertiger technischer Geräte angeboten wurden und Käufer aufgrund der Abbildungen und vage formulierter Texte dachten, sie hätten das Produkt selbst ersteigert und ein echtes Schnäppchen gemacht.

Abofallen und Kostenrisiken bei Apps

Eine beliebte Masche unseriöser Unternehmen waren Abofallen. Vor allem auf Webseiten, auf denen digitale Inhalte angeboten wurden, konnten Besucher mit einem einzigen Klick ein kostenpflichtiges Abonnement abschließen. Häufig verlangten Anbieter dabei für eine magere Gegenleistung heftige Monatsgebühren. Über den genauen Leistungsumfang und den Preis wurden Käufer im Unklaren gelassen, da diese Informationen versteckt waren.

Diesem Gebaren hat der Gesetzgeber 2012 einen Riegel vorgeschoben, seitdem müssen Verbrauchern eindeutige Hinweise auf jeden verbindlichen Kaufvorgang gegeben werden. Eine Verschleierung einer kostenpflichtigen Bestellung ist nicht mehr so einfach möglich. Bei jedem Bestellvorgang in einem Onlineshop muss eine Schaltfläche mit einer Formulierung wie »Kostenpflichtig bestellen«, »Zahlungspflichtig bestellen«, »Kaufen« oder »Jetzt kaufen« vorhanden sein, die ein Kunde zwingend anklicken muss, damit der

NUTZEN SIE SPERREN UND PASSWORTSCHUTZ

Bei Android und iOS gibt es die Möglichkeit, das Herunterladen kostenpflichtiger Software zu reglementieren. Bei Google Play lässt sich dazu ein Passwort festlegen, das für jeden Kauf eingegeben werden muss. Apple-Geräte können für In-App-Käufe sogar komplett gesperrt werden (über *Einstellungen/Einschränkungen/In-App-Käufe*), und auch hier kann ein Passwort für Käufe vorgegeben werden.

Auf iPhones und iPads können Sie In-App-Käufe komplett sperren.

Kaufvertrag zustande kommt. Außerdem müssen Kunden vor dem Abschluss einer Bestellung alle relevanten Produktmerkmale sowie der Gesamtpreis (inklusive etwaiger Zusatzkosten und Versandgebühren) angezeigt werden.

Eine Renaissance erleben Abofallen auf Smartphones, und das gleich in zwei Varianten. Hier geht eine gewisse Gefahr von In-App-Käufen aus, bei denen Nutzer einer App kostenpflichtige Erweiterungen kaufen. Oft sind es Gratisspiele, bei denen Spielfiguren, Zusatzfunktionen und Zusatzlevel hinzugekauft werden müssen. Es gibt zwar meist Hinweise auf die Kosten, allerdings beachten gerade Kinder und Jugendliche diese sehr häufig nicht oder sind sich der finanziellen Auswirkungen nicht wirklich bewusst.

Perfider ist ein Trick, der eine direkte Weiterentwicklung der klassischen Abofalle ist: Beim Anklicken eines Werbebanners in einer App wird eine Internetverbindung zum Anbieter aufgebaut. Dabei wird das alte WAP-Protokoll verwendet, über das auch die Mobilfunknummer des Anschlusses übertragen wird. Der Anbieter kann dem Teilnehmer nun den Aufruf der Seite und weitere Leistungen über das WAP-Billing in Rechnung stellen. Häufig tarnen sich diese kostenpflichtigen Dienste als Gewinnspiele.

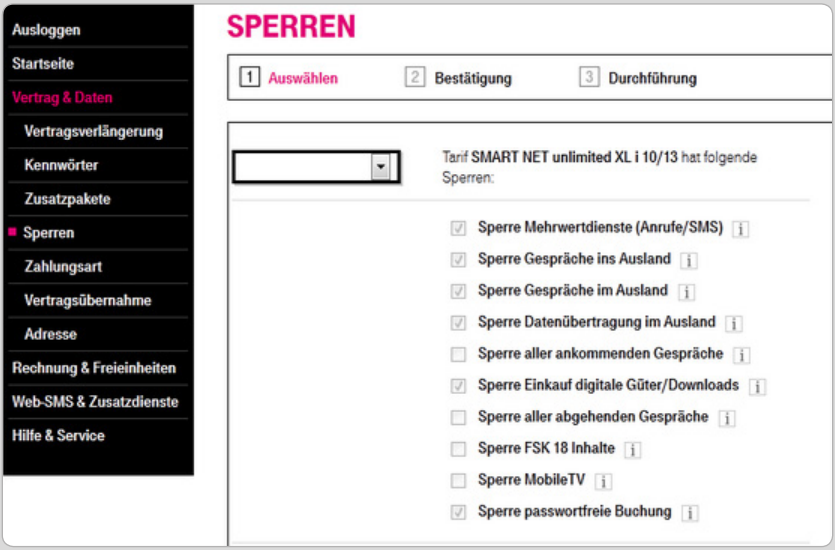
Die Zahlung erfolgt über die Mobilfunkrechnung des Nutzers und wird vom Mobilfunkprovider des Anbieters eingetrieben. Die Rechnung für ein auf diese Weise abgeschlossenes Abo ist damit Teil der Mobilfunkrechnung, und der Provider wird zunächst auf der Zahlung dieses Rechnungspostens bestehen,

da er selbst diesen Betrag (abzüglich einer Provision) an den Anbieter überwiesen hat und nun als Inkasso-Unternehmen auftritt.

Da die meisten Unternehmen, die mit diesem Trick arbeiten, im Ausland ansässig sind, ist es sehr aufwendig, sich dagegen zu wehren und etwa Einspruch gegen den Anbieter zu erheben oder einen Nachweis zum angeblichen Vertragsabschluss anzufordern. Das Kürzen der Mobilfunkrechnung um den umstrittenen Betrag kann auch negative Folgen haben, sodass es schwer ist, ohne großen Aufwand und unbeschadet aus dieser Falle herauszukommen.

RICHTEN SIE EINE SPERRE FÜR MEHRWERTDIENSTE EIN

Den Ärger mit WAP-Billing-Fallen können Sie von vornherein ausschließen, wenn Sie bei Ihrem Mobilfunkanbieter die Nutzung von Mehrwertdiensten komplett sperren lassen. Dann können Sie mit Ihrem Handy oder Smartphone allerdings auch keine seriösen Angebote mit diesem Bezahlmodell mehr nutzen.



Mit einer Sperre für Mehrwertdienste können Sie sich Ärger ersparen.

5.2 Zahlungsmethoden beim Einkaufen im Web

Zum Shoppen im Web gehört leider auch das Bezahlen. Zur Begleichung des Kaufpreises stehen mittlerweile sehr viele Möglichkeiten zur Verfügung, die meisten Onlineshops bieten allerdings nur eine begrenzte Auswahl an.

Klassische Zahlungsverfahren

Auch im Onlinehandel können Sie ganz konventionelle Zahlungsverfahren verwenden. Zu den populärsten gehört der Kauf auf Rechnung. Sie bestellen eine Ware online, und zusammen mit dem Produkt kommt die Rechnung zu Ihnen nach Haus. Sie haben Zeit, das Produkt zu prüfen, und begleichen anschließend den Kaufbetrag innerhalb einer bestimmten Frist etwa durch eine Überweisung von Ihrem Girokonto.

Hier tritt der Onlineshop in Vorleistung, indem er die bestellten Waren liefert und auf die Zahlungsbereitschaft des Kunden vertraut. Allerdings haben die Onlineshops die Möglichkeit, noch direkt während des Bestellvorgangs die Bonität der Kunden durch entsprechende Dienstleister beurteilen zu lassen und zu reagieren. Diese Zahlungsmethode erscheint dann an der virtuellen Kasse einfach nicht mehr. Das kann auch schon dann passieren, wenn Sie das Pech haben, einen schlechten Scoring-Wert bei der Schufa zu besitzen, weil sich zu viele Ihrer Nachbarn als säumige Zahler erwiesen haben.

Ebenfalls konventionell ist die Zahlung per Nachnahme, bei der allerdings zusätzliche Gebühren den Onlinekauf verteuern. Außerdem ist das Verfahren recht umständlich, weil Sie den Betrag direkt beim Paketboten begleichen müssen. Der Schutzeffekt dieser Zahlungsmethode, bei der Kunden ja erst zahlen, wenn die Lieferung tatsächlich eintrifft, sollte nicht überschätzt werden. Denn erst nach der Zahlung lässt sich überprüfen, ob wirklich der bestellte Artikel geliefert wurde oder im Paket nicht doch ein falsches Produkt oder eine andere unliebsame Überraschung enthalten ist.

Eine weitere konventionelle Zahlungstechnik, die sich beim Onlineshopping bewährt hat, ist die Lastschrift. Zu den Vorteilen der Lastschrift gegenüber der Rechnung gehört die größere Bequemlichkeit. Als Kunde müssen Sie während des Bestellvorgangs Ihre Kontodaten einmalig angeben. Haben Sie die Erlaubnis zur Abbuchung erteilt, können Sie in diesem Shop beliebig oft einkaufen, ohne umständlich jedes Mal eine Rechnung begleichen oder ein Überweisungsformular ausfüllen zu müssen.

Außerdem haben Sie als Käufer hier die Möglichkeit, den abgebuchten Betrag wieder zurückzubuchen, wenn es bei der Abwicklung des Kaufs zu Problemen gekommen ist. Genaue Fristen für den Widerruf der Zahlung gibt es nicht, meist ermöglichen Geldinstitute diesen jedoch bis zu sechs Wochen nach der Abbuchung. Unberechtigte Abbuchungen, für die keine Erlaubnis erteilt worden war, können sogar unbegrenzt rückgängig gemacht werden.

Generell sollten Sie vor der Durchführung der Rücklastschrift beim Widerruf des Kaufvertrags dem Händler jedoch die Möglichkeit geben, von sich aus den Kaufpreis zu erstatten. Andernfalls entsteht dem Anbieter durch die Gebühren der Rücklastschrift ein unangemessen hoher Schaden, den er seinerseits zurückfordern kann.

STREUUNG DER KONTODATEN IST EIN POTENZIELLES PROBLEM

Ein möglicher Nachteil dieser Zahlungsmethode ist, dass Sie den Shops zwangsläufig Ihre Kontodaten zur Verfügung stellen müssen. Mit jedem zusätzlichen Onlineshop erhöht sich auch das Risiko, dass Ihre Daten doch einmal in die falschen Hände geraten, etwa wenn die Server eines Anbieters gehackt und Daten gestohlen werden. Das ist zwar nicht an der Tagesordnung, doch hin und wieder passiert so etwas doch einmal. Die erbeuteten Daten können Betrüger anschließend für andere, illegale Zwecke missbrauchen.

Die aus Käufersicht schlechteste konventionelle Zahlungsvariante ist die Vorkasse. Sie bezahlen (etwa per Überweisung) und erhalten die Ware, wenn Ihre Zahlung beim Verkäufer eingegangen ist. Bei großen, seriösen Anbietern ist das Risiko zwar überschaubar, bei unbekannten Anbietern oder in Onlineauktionen sollten Sie jedoch besonders skeptisch sein und vor allem bei größeren Summen zusätzliche Sicherheitsmaßnahmen wie einen Treuhandservice nutzen.

Zahlen per Kreditkarte

Deutschland war lange Zeit im Hinblick auf die Kreditkartennutzung so etwas wie ein Entwicklungsland. Viele Bundesbürger hatten und haben erhebliche Vorbehalte gegen diese Form des Plastikgelds. Im internationalen Vergleich kommen die Karten hierzulande immer noch eher selten zum Einsatz, wenngleich die Akzeptanz in den letzten Jahren deutlich gestiegen ist.

Das Zahlen per Kreditkarte in Onlineshops hat gegenüber den eben beschriebenen Methoden einige Vorteile. So ist es deutlich unkomplizierter und schneller als eine Überweisung. Als Käufer geben Sie lediglich Kartengesellschaft und Kartennummer sowie die Sicherheitsnummer ein. Die Daten werden direkt auf Plausibilität überprüft, und der Verkäufer gelangt schnell an sein Geld. Kreditkartenzahlung wird gern für den Kauf digitaler Waren (Software, Video- und Audio-Downloads etc.) oder beim Bezahlen von Tickets verwendet.

Die Kreditkarte wird auch beim Onlineshopping immer öfter genutzt.

Andererseits sind mit dieser einfachen Zahlungsmethode auch einige Probleme verbunden: Sind Betrüger im Besitz Ihrer Kreditkartendaten, können sie auf Ihre Kosten einkaufen. Der einzige Lichtblick ist dann, dass Sie den Schaden meist relativ problemlos erstattet bekommen, wenn Sie sich nicht fahrlässig verhalten haben.

VORSICHT VOR KREDITKARTENDATEN-PHISHING

Kreditkartendaten sind bei Internetganoven besonders begehrt. Über Phishing-Attacken wird immer wieder versucht, Karteninhaber zur Preisgabe dieser Informationen zu bewegen. Es gibt aber auch viele Versuche, die Server von Onlineshops oder anderen Onlinediensten zu knacken und die Kundendaten inklusive der Kreditkarteninformationen zu stehlen.

Eine neue Schutzvorkehrung soll das Bezahlen per Kreditkarte in Webshops sicherer machen. Dabei werden bei dem Geldinstitut, das die Kreditkarte ausgibt, ein zusätzliches Kennwort in Form einer persönlichen Begrüßung sowie eine Geheimnummer (PIN) vereinbart. Beim Zahlungsvorgang im Internet wird der Kartennutzer dann auf eine Webseite geleitet, auf der diese persönliche Begrüßung angezeigt wird. Stimmt die Begrüßung mit der Vereinbarung überein, kann der Zahlungsvorgang durch die Eingabe der PIN abgeschlossen werden.

Bei dieser Option, die bei MasterCard *SecureCode* heißt, laufen Phishing-Angriffe ins Leere, da Betrüger die persönliche Begrüßungsformel nicht kennen und sie ja auch nicht vom Nutzer eingegeben werden muss, sodass sie nicht per Spyware ausspioniert werden kann. Auf der gleichen Basis funktioniert die Sicherheitstechnik 3-D Secure, die von der Kreditkartenorganisation VISA entwickelt wurde und ebenfalls die Eingabe eines zusätzlichen Codes vorsieht.

Giropay und Sofortüberweisung.de

Onlinebanking-Nutzer haben seit einiger Zeit die Möglichkeit, bei Überweisungen den Informationsfluss zu beschleunigen. Bei diesen Systemen wird dem Shopbetreiber direkt nach der Onlineüberweisung signalisiert, dass der Kunde die Ware bezahlt hat, sodass er seine Ware ohne Risiko unmittelbar versenden oder online verfügbar machen kann. Der Händler muss also nicht warten, bis sein Institut ihm den Betrag auf seinem Konto gutgeschrieben hat.

Beim Giropay-Verfahren gelangen Sie von der Bezahlseite des Onlineshops nach Eingabe der Bankleitzahl Ihres Instituts auf dessen Website und nehmen wie üblich per PIN und TAN die Überweisung vor. Danach kehren Sie automatisch zum Onlineshop zurück. Das Verfahren hat für Sie den Vorteil, dass an den Händler außer der Bankleitzahl keine weiteren Kontodaten übermittelt werden, da der eigentliche Bezahlvorgang auf der Bank-Website stattfindet.

Giropay beschleunigt die Abwicklung des Kaufvorgangs.

Giropay wird unter anderem von der Postbank, der Commerzbank, vielen Sparkassen und Genossenschaftsbanken sowie einigen kleineren Instituten angeboten, andere Branchengrößen haben sich diesem System jedoch nicht angeschlossen.

Diese Lücke im Angebot will das System *Sofortüberweisung.de* schließen, das eine ähnliche Vorgehensweise bietet wie Giropay. Hier gibt der Käufer PIN

und TAN nicht auf den Webseiten seiner eigenen Onlinebank ein, sondern bei Sofortüberweisung.de. Hat man dort die Daten hinterlegt, folgt der Zugriff auf das Konto bei der eigenen Onlinebank. Diese Praxis verstößt allerdings gegen die AGB vieler Onlinebanken, die die Weitergabe der Zugangsdaten (PIN und TAN) an Dritte strikt untersagen, um sich dadurch bei Missbrauchsfällen gegen eine Übernahme der Schäden wehren zu können. In der Praxis ist es nach Angaben des Betreibers bislang jedoch noch nie zu einem Missbrauch gekommen, zudem unterwirft sich das Unternehmen auch regelmäßigen Sicherheitsüberprüfungen, etwa durch den TÜV Saarland oder andere unabhängige Sicherheitsunternehmen. Fakt bleibt aber, dass Nutzer hier Zugangsdaten zu Ihren Konten in fremde Hände geben.

PayPal

PayPal ist zwar ein Tochterunternehmen des Auktionshauses eBay, über diesen Bezahldienst können Kunden aber auch in zahlreichen anderen Onlineshops bezahlen. Bei PayPal handelt es sich um ein lizenziertes Kreditinstitut, das den strengen Auflagen der Finanzdienstleistungsbehörden unterliegt. Als Kunde von PayPal richten Sie dort ein Konto ein, das Sie auf unterschiedlichen Wegen, etwa per Lastschrift, über die Kreditkarte oder auch via Giropay, nach einem Kauf automatisch ausgleichen können. Außerdem lässt sich das Konto per Überweisung vorab mit einem Guthaben auffüllen.

Das Zahlen per PayPal ist einfach und sicher.

Zum Bezahlen per PayPal in einem Onlineshop werden Sie als Käufer direkt auf die PayPal-Seite geleitet, auf der Sie sich mit Ihrer E-Mail-Adresse und einem Passwort einloggen und die Überweisung per Mausklick vornehmen. Im Vergleich zur direkten Bezahlung hat PayPal den Vorteil, dass Sie Ihre Konto- und Kreditkartendaten nur bei PayPal angeben müssen und nicht bei jedem einzelnen Onlineshop, in dem Sie einkaufen. Zudem informiert PayPal den Shopbetreiber direkt über die erfolgte Zahlung, sodass die Kaufabwicklung im

Vergleich zur Überweisung oder zur Lastschrift beschleunigt wird. Für Käufe bei eBay ist mit PayPal ein Käuferschutz verbunden.

VORSICHT VOR PAYPAL-PHISHING

Der Erfolg und die Einfachheit von PayPal führen dazu, dass dieses System verstärkt im Fokus von Phishing-Angriffen steht. Auf nachgestellten Webseiten, auf die Sie durch E-Mails gelockt werden, versuchen Betrüger, Ihre Zugangsdaten in Erfahrung zu bringen. Zum besseren Schutz bietet PayPal weitere Sicherungsmaßnahmen, dabei müssen Sie sich zusätzlich über eine temporär gültige Geheimnummer ausweisen. Diese Nummer können Sie sich kostenfrei per SMS zuschicken lassen oder durch einen Generator im Scheckkartenformat erzeugen.

Prepaid-Zahlungssysteme

Beim Bezahlen kleinerer Beträge kommen häufig Prepaid-Systeme zum Einsatz. Die haben den Vorteil, dass die anfallenden Transaktionskosten gering sind und auch kleinere Beträge wirtschaftlich abgerechnet werden können. Bei dieser Art des Bezahlens kann der Käufer anonym bleiben.

Paysafecard hat sich unter den Prepaid-Systemen durchsetzen können.

Zu den bekanntesten Systemen, für das es auch vergleichsweise viele Akzeptanzstellen gibt, gehört Paysafecard. Sie können an über 50.000 Verkaufsstellen (z. B. Tankstellen, Supermärkten etc.) oder auf der Paysafecard-Website ein Guthaben erwerben (10 bis 100 Euro). Dafür gibt es einen 16-stelligen PIN-Code, der beim Bezahlen in ein Webformular eingegeben wird. Der fällige Rechnungsbetrag wird vom Guthaben abgezogen. Von Vorteil bei Paysafecard ist, dass das Verlustrisiko automatisch auf den Restbetrag des Guthabens beschränkt ist.

Um nicht immer ein Guthaben bis auf den letzten Cent aufbrauchen zu müssen, können Sie mehrere Guthabenkarten (maximal zehn) miteinander verknüpfen. So lassen sich zugleich auch größere Beträge bezahlen. Mit der Paysafecard sind sogar Zahlungen in Fremdwährungen möglich. Mittlerweile gibt es auch eine App, mit der einfach durch Scannen eines QR-Codes im Webshop gezahlt werden kann.

Andere Prepaid-Zahlungssysteme haben bei Weitem nicht die Verbreitung von Paysafecard. Vor einigen Jahren hat die Telekom ihr Angebot MicroMoney eingestellt, sodass es nur noch wenige Alternativen gibt. Am bekanntesten sind Wirecard-Guthabenkarten, die es in Versionen der Kreditkartenunternehmen VISA und Mastercard gibt. Mit diesen Guthabenkarten, die per Überweisung aufgefüllt werden, können Sie überall bezahlen, wo diese Kreditkarten in der Originalversion akzeptiert werden. Durch das Prepaid-Prinzip ist das Verlustrisiko bei Missbrauch auf das Guthaben beschränkt.

ZAHLUNGS-VERFAHREN	WESENTLICHE VOR- UND NACHTEILE AUS KUNDENSICHT
Rechnung (Überweisung)	Zahlung erst nach Erhalt der Ware, wird für digitale Güter und Kleinbeträge oftmals nicht angeboten, etwas umständlich.
Lastschrift	Bequemes Zahlverfahren, Rückbuchungsmöglichkeit vorhanden, jeder Onlineanbieter erhält Kontodaten.
Nachnahme	Relativ umständliches und teures Verfahren, keine wirkliche Kontrollmöglichkeit vor der Bezahlung.
Vorkasse	Hohes Risiko beim Kauf, nur bei sehr seriösen und renommierten Anbietern nutzen, um Folgekäufe eventuell mit anderen Zahlungsoptionen durchführen zu können.
Kreditkarte	Relativ einfach und bequem, jeder Onlineanbieter erhält Kreditkartendaten, populäres Ziel für Phishing-Angriffe.
Giropay	Beschleunigt die Abwicklung des Kaufvorgangs, Händler erhalten keine Kontodaten, nicht bei allen Banken nutzbar.
Sofortüberweisung.de	Beschleunigt die Abwicklung des Kaufvorgangs, Händler erhalten keine Kontodaten, Zugangsdaten zum Onlinekonto und TAN werden jedoch dem Betreiber dieses Zahlungsdiensts anvertraut.
PayPal	Relativ universell einsetzbare Zahlungsmethode, viele Akzeptanzstellen, Händler erhalten keine Kontodaten, populäres Ziel für Phishing-Angriffe.
Prepaid-Karten	Ideal für schnelle Bezahlung von digitalen Gütern und sofort verfügbaren Onlinedienstleistungen, teilweise anonyme Bezahlmöglichkeit, etwas umständlich durch begrenztes Guthaben.

6 SICHERHEIT BEI DER MOBILEN INTERNETNUTZUNG

Noch vor wenigen Jahren erfolgte der Zugang zum Internet nahezu ausschließlich per Desktop oder Notebook zu Hause oder im Büro, nur wenige Businessanwender surften auch unterwegs per Mobilfunkanbindung. Etwas flexibler wurde der Zugang durch WLAN und schnelle Mobilfunktechniken wie UMTS oder LTE. Nochmals deutlich verändert hat sich das Nutzungsverhalten durch neue Mobilgeräte wie Smartphones und Tablets. Mit der mobilen Internetnutzung hat sich aber auch die Gefahrenlage verändert.

6.1 Gefahrenlage für Smartphones und Tablets

Wenn Sie mit Tablet oder Smartphone online gehen, gibt es prinzipiell erst einmal eine gute Nachricht. Das Risiko, dass Sie zum Opfer eines Virenangriffs werden, ist gering. Die meisten Angriffe mit Schadsoftware zielen immer noch auf Windows-Rechner, andere Systeme sind deutlich weniger betroffen. Werden auf mobilen Plattformen Schwachstellen entdeckt, hat dies daher keine so gravierenden Folgen wie im PC-Bereich, wo Lücken sofort für Angriffe ausgenutzt werden.

Allerdings gilt dies nur mit einer gewissen Einschränkung. So gibt es bereits eine nennenswerte Zahl von Schadprogrammen für Android, deshalb sollten Sie auf Android-Tablets und -Smartphones, wie auf Windows-Rechnern, eine Antivirensoftware verwenden. Zudem gibt es auf allen Plattformen einige Gefahren für Ihre Privatsphäre, da neugierige Apps viel mehr von Ihnen preisgeben, als Sie eigentlich wollen. Auch Phishing-Angriffe, bei denen Sie nach Zugangsdaten ausgefragt werden, finden unabhängig vom jeweiligen System statt.

Die grundlegenden Schutzmaßnahmen, die Sie für die verschiedenen Mobilplattformen ergreifen sollten, haben wir Ihnen bereits in Kapitel 2 dieses Buchs vorgestellt, sodass wir hier nur eine kurze Zusammenfassung geben und auf einige aktuelle Entwicklungen eingehen.

Windows Phone 8 und iOS

Keine besonderen zusätzlichen Anstrengungen müssen Sie als Nutzer von Apple-iOS-Geräten oder Smartphones mit Windows Phone 8.x unternehmen. Diese Plattformen sind sicher, und solange Sie Software nur direkt aus den offiziellen App-Stores installieren, ist das Risiko minimal. Beide Systeme sind

so voreingestellt, dass ohne Weiteres auch gar keine andere Software auf die Geräte gelangen kann. Erst durch Jailbreaking kann diese Einschränkung aufgehoben werden, was zusätzliche Gefahren birgt.

Ansonsten sollten Sie die Optionen zur Gerätesperre nutzen, wichtige Daten zusätzlich verschlüsseln und bei der Installation neuer Apps darauf achten, welche Rechte sie einfordern und auf welche Daten und Dienste sie zugreifen. Registrieren Sie das Gerät außerdem bei den Herstellerdiensten zum Auffinden und Fernlöschen, haben Sie die wichtigsten Sicherungsmaßnahmen durchgeführt.

Android

Wie bereits mehrfach erwähnt, ist Android sicherheitstechnisch unter den Mobilplattformen das große Sorgenkind. Dies liegt daran, dass auch Software aus anderen Quellen installiert werden kann, was sich Entwickler von Schadsoftware zunutze machen, indem sie versuchen, Trojaner auf die Geräte zu schmuggeln. Beispielsweise werden Nutzer per Kurznachricht oder E-Mail dazu aufgefordert, eine Treiberaktualisierung oder ein Sicherheitsupdate vorzunehmen, oder es wird ein anderer Vorwand genutzt, um eine Software zu überspielen.

Android hat aber noch andere Defizite. So gibt es hier anders als bei den anderen Plattformen keine einheitliche Update-Politik. Je nach Gerätehersteller werden die von Google entwickelten Firmware-Updates an die Nutzer ausgeliefert oder eben nicht. Dasselbe gilt auch für Sicherheitspatches, die Google

AUFPASSEN BEI ÄLTEREN ANDROID-VERSIONEN

Schwachstellen in den alten Android-Versionen werden nicht mehr geschlossen. Ein aktuelles und zugleich gravierendes Beispiel ist die UXSS-Schwachstelle, über die Angreifer vertrauliche Daten ausspionieren können. Von dieser Sicherheitslücke sind alle Android-Geräte betroffen, die mit einer Version bis einschließlich Android 4.3 ausgestattet sind. Ursache des Problems ist ein Fehler im Android-Browser, genauer gesagt, in der Web-View-Komponente. Diese wird nicht nur beim integrierten Webbrowser verwendet, auch zahlreiche andere Apps greifen darauf zu, um Webinhalte darzustellen.

Im Internet gibt es einen Test zur USXX-Sicherheitslücke.

für seine Betriebssysteme anbietet. Gerade bei älteren und billigeren Android-Geräten müssen die Anwender häufig auf eine Aktualisierung verzichten und sich mit veralteten Android-Versionen begnügen.

Da Google angekündigt hat, keine Sicherheitspatches für alte Versionen anzubieten, müssen Sie bei der Nutzung einer solchen Hardware besonders vorsichtig sein. Wenn ein Umstieg auf Android 4.4 oder höher möglich ist, sollten Sie davon Gebrauch machen. Ist das nicht möglich, sollten Sie unbedingt auf einen anderen Browser umsteigen. Allerdings muss es sich dabei um einen Browser mit eigener Rendering-Engine handeln. Damit kommen etwa Firefox, Chrome oder Dolphin infrage.

6.2 Öffentliches WLAN: Nutzen und Risiken

Für die mobile Internetnutzung kommen zwei Varianten infrage. Zum einen können Sie Ihre Mobilfunkverbindung verwenden, zum anderen stehen Ihnen an zahlreichen Orten auch öffentliche WLANs zur Verfügung. Beide Möglichkeiten haben Stärken und Schwächen. Moderne Mobilfunknetze wie UMTS und LTE haben hinsichtlich der Geschwindigkeit zwar deutlich aufgeholt, oftmals wird die Bandbreite aufgrund der hohen Zahl von Nutzern in einer Funkzelle für die einzelnen Nutzer jedoch wieder stark beschnitten, sodass WLAN-Anschlüsse meist schneller sind. Zudem sind längst nicht alle Smartphones und Tablets schon mit den schnellsten Mobilfunkvarianten ausgerüstet, sondern bieten häufig noch eine langsamere Technik, sodass der Unterschied zum Surfen per WLAN oft noch größer ist.

Zudem gibt es im Hinblick auf die Kosten der Internetnutzung Unterschiede. Zwar kostet das Surfen per Mobilfunk schon seit einiger Zeit kein Vermögen mehr, und einfache Surf-Flatrates für Smartphones und Tablets gibt es zu moderaten Preisen, doch sollten Sie sich von der Bezeichnung Flatrate nicht täuschen lassen.

Sie können für einen monatlichen Festpreis unbegrenzt Daten übertragen, jedoch steht Ihnen dabei die maximale Geschwindigkeit nur für ein begrenztes Datenvolumen zur Verfügung. Überschreiten Sie dieses Limit, wird der Anschluss verlangsamt, und bei Übertragungsraten aus der Modemsteinzeit ist

nur noch eine eingeschränkte Nutzung möglich. Je höher dieses Datenlimit angesetzt ist, desto teurer wird auch der Mobilfunkvertrag. Angesichts der hohen Datenmengen, die beim normalen Surfen mittlerweile anfallen, sollte diese Grenze nicht zu knapp bemessen sein.

Öffentliche, unverschlüsselte WLANs sind populär, bergen aber Risiken.

Das Surfen an öffentlichen WLANs kommt dagegen ohne derartige Einschränkungen aus. Es gibt auch viele freie WLANs, die für jedermann oder bestimmte Gruppen (z. B. für Gäste von Hotels oder Cafés) kostenlos nutzbar sind. Auch einige große Mobilfunkunternehmen unterhalten ein Netz mit WLAN-Zugängen, die für die eigenen Kunden ohne Zusatzkosten oder einen geringen Aufpreis nutzbar sind.

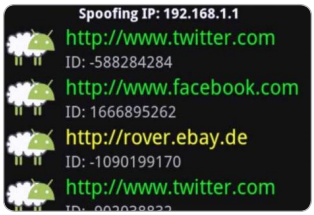
Den Kostenvorteil können WLANs vor allem auch im Ausland ausspielen, denn die Kosten für das Datenroaming im Mobilfunk sind immer noch recht hoch, und längst nicht immer gibt es Pauschaltarife, sondern jedes MByte muss extra bezahlt werden. Auch kann WLAN gerade in ländlicheren Regionen noch mit Geschwindigkeitsvorteilen aufwarten, da dort noch ältere Mobilfunknetze zu finden sind, die nur sehr geringe Bandbreiten bieten.

Allerdings ist die Nutzung öffentlicher WLAN-Zugänge mit einigen Gefahren verbunden. So lassen sich Datenübertragungen an offenen WLAN-Hotspots sehr einfach abhören. Längst bedarf es dazu keiner Profiausrüstung mehr, und es gibt zahlreiche Tools, mit denen sich jeder Interessierte als Hobbyspion versuchen kann.

Zu den bekanntesten Abhörtools gehört DroidSheep. Die App läuft auf Android-Hardware und ermöglicht es, im Datenstrom des WLAN nach Zugangsdaten in Form von Session-Cookies zu suchen. Mit diesen Cookies identifiziert sich ein Clientrechner, solange er bei einem Dienst eingeloggt ist. Kommt ein Angreifer in den Besitz dieser Session-Cookies, kann er die Identität des Opfers übernehmen und bekommt so ebenfalls einen Zugang zu diesem Dienst. Auf diese Weise könnte also der Herr am Tisch nebenan mit seinem Smartphone während des Hotelfrühstücks Ihr E-Mail- oder Facebook-Konto nutzen und dort Nachrichten posten oder Mails verschicken.

Unter professionelleren Hackern hat sich ein weiterer Trick etabliert: Sie stellen eigene WLAN-Hotspots auf, über die sie den Datentransfer der Nutzer aufzeichnen. Ein solcher WLAN-Hotspot lässt sich mit einfachen Mitteln

realisieren, es reicht schon ein konventionelles Smartphone aus, das seinen Mobilfunkinternetzugang per WLAN für andere Geräte zur Verfügung stellen kann. Noch professioneller lässt sich ein solches WLAN mit einem Notebook samt externem WLAN-Adapter aufbauen. Externe WLAN-Module besitzen eine hohe Sendeleistung und erreichen damit eine beachtliche Reichweite, das Notebook wiederum stellt per Mobilfunkadapter den Zugang zum Internet bereit.



Schon mit einfachen, frei verfügbaren Apps kann der Datenverkehr im unverschlüsselten WLAN abgehört werden.

Damit diese WLANs keinen Verdacht erregen, tarnen Hacker ihre Hotspots, indem sie ihnen ganz vertraut klingende Namen geben. Diese WLAN-Namen (SSID – *Service Set Identifier*) senden alle Zugangspunkte und Hotspots aus, um sich zu erkennen zu geben. Die meisten Endgeräte verbinden sich automatisch mit dem stärksten WLAN gleichen Namens. Sitzt also ein Datenspion im Hotel im gleichen Raum nur wenige Meter entfernt von Ihnen und hat auf seinem Smartphone oder Notebook einen WLAN-Zugangspunkt unter derselben SSID wie das echte WLAN des Hotels eingerichtet, landen Sie unter Umständen auf seinem Rechner und nicht beim eigentlich beabsichtigten Zugang.

KONTROLLIEREN SIE DIE ANMELDESEITE BEI ÖFFENTLICHEN WLAN-HOTSPOTS

Wenn Sie über einen nachgestellten Hotspot ins Internet gehen, kann der Angreifer den Datenstrom überwachen. Um nicht aufzufallen, ahmen die Datenspione oftmals auch eine eventuell vorhandene Willkommensseite des nachgeahmten WLAN-Hotspots nach. Häufig wird dieser Trick sogar verwendet, um Kreditkartendaten abzufangen. Dies geschieht, indem die Hotspot-Nutzer zunächst eine Seite angezeigt bekommen, auf der sie auf die Kosten der Hotspot-Nutzung hingewiesen und zwecks Abrechnung nach ihren Kreditkartendaten gefragt werden.

Nicht immer verwenden Angreifer genau den gleichen Namen, in vielen Fällen wird auch ein Hotspot mit einer ähnlichen SSID verwendet. Denn die meisten Nutzer werden froh sein, wenn sie ein frei zugängliches WLAN finden, und kaum zögern, sich damit zu verbinden.

Die Umleitung des Datenverkehrs kann auch über das ARP-Spoofing (ARP steht für *Address Resolution Protocol*) ablaufen. Dieses Angriffsszenario wird von professionellen Hackern verwendet und ist aufwendiger als die Einrichtung eines einfachen WLAN-Hotspots. Die Methode kommt auch in Firmennetzen oder anderen lokalen Netzen zum Einsatz, wo Eindringlinge ihre Geräte damit als reguläre Hotspots oder Access Points des Firmennetzes tarnen. Im Endeffekt laufen beide Varianten allerdings auf dasselbe hinaus, nämlich darauf, dass der Datenaustausch nicht über die regulären WLAN-Zugangspunkte läuft, sondern über die Geräte der Datenspione, die auf den Datenfluss zugreifen.

7 DATENSICHERHEIT IN DER CLOUD

Cloudspeicherdienste sind vor allem durch die zunehmende Nutzung von Smartphones und Tablets populär geworden. Um von unterschiedlichen Endgeräten aus jederzeit auf Daten zugreifen zu können, sind diese Angebote ideal. Außerdem sind die Speicherkapazitäten vieler Mobilgeräte beschränkt, sodass eine Auslagerung von Daten in die Cloud ohnehin notwendig wird. Allerdings sollten Sie bei der Nutzung daran denken, dass Daten sowohl auf dem Übertragungsweg als auch auf dem Cloudspeicher vor dem Zugriff durch Dritte geschützt sein sollten.

7.1 Cloudspeicher mit Verschlüsselung

Auf Cloudservern landen immer mehr Daten, und darunter befinden sich früher oder später auch Dokumente, die nicht für die Augen Dritter bestimmt sind. Die Daten sind nicht nur auf dem Übertragungsweg, sondern auch auf dem Cloudspeicher selbst gefährdet. Hacker könnten die Datenspeicher angreifen und Informationen stehlen, aber auch unzuverlässige Mitarbeiter der Cloudanbieter könnten sich Zugang verschaffen. Dazu kommen die weitreichenden Befugnisse von Geheimdiensten und anderen staatlichen Stellen, die speziell in den USA kaum noch Grenzen kennen. Spätestens seit den Snowden-Enthüllungen ist die umfassende Zusammenarbeit der meisten großen Internetkonzerne mit den Geheimdiensten bekannt.

TRANSPORTSICHERUNG IST MEIST VORHANDEN

Die Sicherung der Daten auf dem Transportweg zwischen Cloudserver und den Clientrechnern ist in der Praxis kein großes Problem, hier bietet eigentlich jeder Clouddienst eine Verschlüsselungslösung an. Meist handelt es sich dabei um die bekannte SSL-/TLS-Verschlüsselung, die auch auf vielen Webseiten zum Einsatz kommt.

Bei der Datenspeicherung auf den Servern gibt es erhebliche Unterschiede. Viele Anbieter haben gar keine Verschlüsselungslösung vorgesehen, einige versprechen eine zuverlässige Verschlüsselung. Gerade bei den besonders populären Diensten großer Anbieter wie Dropbox, Microsoft (OneDrive) oder Google (Google Drive) fehlt dieser Service. Bei US-Unternehmen kommt wie erwähnt noch hinzu, dass NSA und andere Dienste sich jederzeit Zugriff auf die

Daten verschaffen können. Auf europäischen Servern und bei europäischen Anbietern sind Daten vor derartigen Zugriffen noch etwas besser geschützt. Viele Unternehmen werben mittlerweile daher mit der Datensicherheit in der EU und dem Hinweis auf europäische Serverstandorte.

Verschlüsselte Cloudspeicher

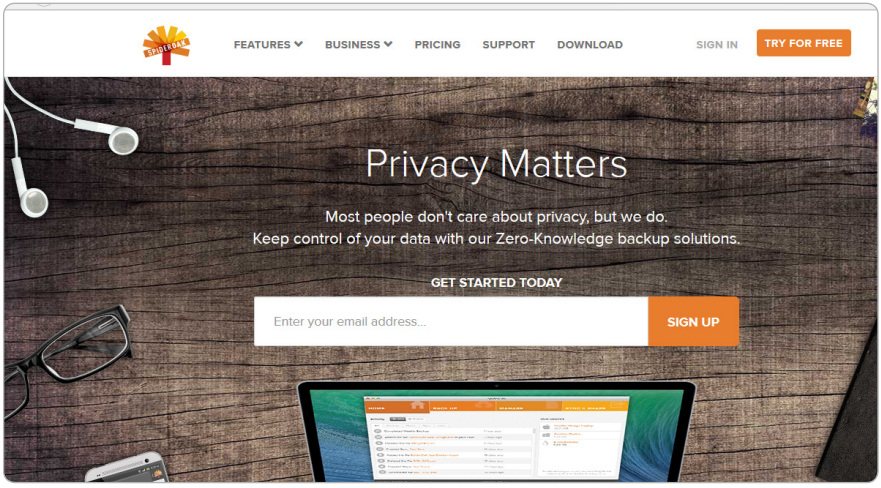
Zu den bekanntesten Cloudanbietern mit einer echten Ende-zu-Ende-Verschlüsselung gehört Wuala, das ursprünglich vom Schweizer Festplattenhersteller LaCie gegründet wurde. Obwohl der US-Konzern Seagate zwischenzeitlich das Unternehmen übernommen hat, stehen die Cloudspeicher immer noch ausschließlich in europäischen Ländern (Schweiz, Deutschland und Frankreich) und sollen so sicher sein vor dem Zugriff durch amerikanische und britische Geheimdienste.

Wuala gehört zu den wenigen Cloudspeicherdiensten mit integrierter Verschlüsselung.

Ob die Verschlüsselung wirklich hundertprozentig sicher ist, lässt sich allerdings nicht eindeutig beantworten, denn das Unternehmen hat den Quellcode der Software nicht vollständig veröffentlicht, sodass er nicht von unabhängigen Experten geprüft werden kann. Dieses Problem betrifft aber prinzipiell alle Verschlüsselungslösungen, sofern sie nicht als Open Source offengelegt werden.

Die Nutzung von Wuala ist mit einer Clientsoftware von allen wichtigen Plattformen aus möglich. Neben Versionen für Windows, Mac OS X und Linux werden auch Android und iOS unterstützt. 2014 hat das Unternehmen sein Gratisangebot abgeschafft. Seitdem gibt es das Einsteigerpaket mit 5 GByte für 0,99 Euro im Monat (oder 9 Euro bei jährlicher Zahlungsweise). 20 GByte kosten 2,99 Euro monatlich (oder 29 Euro jährlich), und 50 GByte sind für 5,99 Euro zu bekommen (65 Euro pro Jahr). Es sind auch deutlich größere Kapazitäten bis zu 2 TByte im Angebot.

Als sehr sicher stufen Experten auch die Cloudlösung von SpiderOak ein, obwohl es sich um einen US-Anbieter handelt, dessen Server auch in den USA stehen. Das System ist etwas komplizierter in der Bedienung, was allerdings primär auf die hohen Sicherheitsstandards zurückzuführen ist. Dazu gehört auch, dass das Passwort für die Verschlüsselung dem Betreiber nicht bekannt ist. Mit diesem Zero-Knowledge-Prinzip wird sichergestellt, dass nicht einmal Mitarbeiter des Unternehmens auf die Daten zugreifen können, selbst wenn sie dazu gezwungen würden. Nachteilig an dem Verfahren ist allerdings, dass ein Nutzer für sein Passwort ausschließlich selbst zuständig ist und es nicht einfach vom Betreiber anfordern kann, sollte er es einmal vergessen haben.



Bei SpiderOak hat der Schutz der Daten oberste Priorität.

Wegen der hohen Sicherheitsstandards hat sogar der Whistleblower Edward Snowden die Nutzung dieses Diensts empfohlen. Angeboten wird er über

Anwendungen und Apps für alle wichtigen Desktop- und Mobilplattformen. SpiderOak bietet eine Speicherkapazität von 2 GByte kostenfrei an, 30 GByte kosten 7 US-Dollar pro Monat.

Allerdings scheinen sich die aufwendigen Sicherheitslösungen für einige Cloudanbieter nicht immer zu rechnen. So musste etwa das deutsche Unternehmen CloudSafe seinen Dienst im Herbst 2014 schon wieder einstellen.

7.2 Verschlüsselungsprogramme

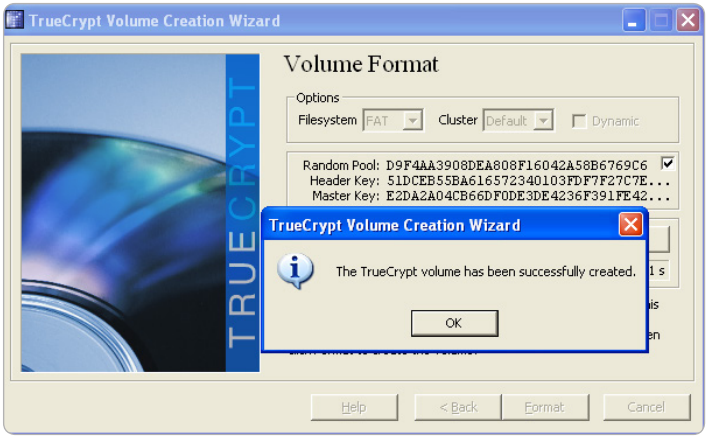
Sie müssen nicht unbedingt einen Cloudspeicher mit integrierter Verschlüsselung verwenden, um Ihre Daten abhörsicher auf den Servern abzulegen. Eine echte Ende-zu-Ende-Verschlüsselung wird auch mit Verschlüsselungsprogrammen möglich, die Sie auf Ihrem Rechner verwenden. Allerdings sind diese Lösungen meist etwas aufwendiger, denn hier müssen Sie ja selbst die Verschlüsselung vornehmen und lagern diese Aufgabe nicht an den Cloudbetreiber aus.

Allgemeine Verschlüsselungsprogramme

Im Prinzip können Sie mit beliebigen Verschlüsselungslösungen Ihre Dateien verschlüsseln, um sie anschließend in die Cloud zu übertragen. Zu den bekanntesten Programmen dieser Art gehört TrueCrypt, das lange Zeit als besonders sicher eingestuft wurde und allgemein als sehr zuverlässig galt. Der Sourcecode von TrueCrypt war weitgehend bekannt, sodass die Sicherheit dieser Lösung auch von unabhängigen Fachleuten überprüft werden konnte. Allerdings haben die Entwickler dieses nicht kommerziellen Programms das Projekt inzwischen eingestellt, und TrueCrypt wird nicht mehr weiterentwickelt.

Zum Zeitpunkt der Einstellung des Projekts kamen Gerüchte auf, dass mit TrueCrypt keine sichere Verschlüsselung mehr möglich sei, allerdings gibt es bislang keine überprüfbaren Belege für derartige Behauptungen. Viele Experten teilen diese Bedenken nicht und empfehlen das Programm nach wie vor zur Verschlüsselung. Dabei sollte allerdings die letzte vollwertige TrueCrypt-Version 7.1a verwendet werden, die später noch angebotene Version 7.2 bietet dagegen nur einen eingeschränkten Funktionsumfang. Auf der Grundlage von TrueCrypt wird derzeit an einem Nachfolgeprogramm gearbeitet, das unter dem Namen Veracrypt angeboten werden soll.

Das Funktionsprinzip von TrueCrypt, das mit Containern arbeitet, in denen die Dateien verschlüsselt werden, ist allerdings nicht auf die Zusammenarbeit mit Cloudspeichern optimiert. In der Praxis kann das einige Probleme bei der Synchronisierung der Daten bereiten. Andere Anwendungen sind in dieser Hinsicht besser geeignet, bieten mehr Komfort und eine einfachere Bedienung.



TrueCrypt ermöglicht eine zuverlässige Verschlüsselung, ist aber nicht besonders komfortabel.

Eine simple Methode, mit der Sie einzelne Dateien verschlüsseln können, gibt es mit dem Archivierungswerkzeug 7-Zip. Das Programm arbeitet mit der sicheren AES-Verschlüsselung, allerdings gibt es auch hier wie bei TrueCrypt keine spezielle Anbindung an Clouddienste, sodass diese Lösung nur dann geeignet ist, wenn Sie wenige Dateien verschlüsseln wollen.

Verschlüsselungsprogramme speziell für Cloudspeicher

Eine Verschlüsselungslösung, die speziell auf die Anforderungen der Cloudnutzung hin entwickelt wurde, ist SafeMonk. Die Software stammt vom renommierten amerikanischen Sicherheitsunternehmen SafeNet und kann von Privatanwendern kostenlos genutzt werden. Das Programm arbeitet allerdings ausschließlich mit dem Cloudspeicherdienst Dropbox zusammen. In diesen Speicherdienst ist die Lösung perfekt integriert. Es wird ein spezieller, verschlüsselter Ordner in der Dropbox angelegt. Alle hierhin verschobenen Dateien werden automatisch schon auf dem Rechner des Anwenders verschlüsselt und dann mit dem Cloudspeicher synchronisiert. Die Schlüssel

verbleiben auch bei SafeMonk ausschließlich bei den Nutzern, sodass der Betreiber die Daten nicht entschlüsseln kann, wenn er es denn wollte. Die SafeMonk-Software gibt es für Windows und Mac OS X sowie für die Mobilplattformen Android und iOS.

SafeMonk zeichnet sich durch Sicherheit und einfachste Bedienung aus.

Die bekannteste Verschlüsselungslösung für die Cloud ist das vom deutschen Unternehmen Secomba angebotene Boxcryptor. Anders als bei SafeMonk ist hier nicht nur die Verschlüsselung auf einem Clouddienst möglich, zusätzlich arbeitet Boxcryptor anstandslos mit sehr vielen populären Speicherlösungen wie CloudMe, GMX Media Center, Google Drive, Microsoft OneDrive und Telekom Cloud zusammen.

Das Programm gibt es mittlerweile in zwei Versionen: in der Classic-Version, deren Verschlüsselungskomponente allerdings zuletzt von Sicherheitsexperten etwas angezweifelt wurde, sowie in der Version Boxcryptor 2.0, die mit einer etwas anderen Technik arbeitet. Für Privatanwender sollte derzeit die Classic-Version noch ausreichen, denn es muss schon ein aufwendiger und zielgerichteter Angriff erfolgen, um diese Verschlüsselung zu knacken. Allerdings bietet die Version 2.0 einige weitere Vorteile. So können Sie mit Boxcryptor 2.0 auch verschlüsselte Dateien für andere Nutzer freigeben, ohne dass Sie diesen zugleich das Passwort mitteilen müssen, wie es in der Classic-Version notwendig ist.

Für beide Varianten gibt es ein Gratisangebot für Privatanwender, das allerdings einige Einschränkungen aufweist. Bei Boxcryptor 2.0 ist die Nutzung mit nur einem Speicherdienst möglich, und es können nur zwei Geräte genutzt werden. Für 36 Euro im Jahr entfallen diese Beschränkungen, außerdem verschlüsselt das Programm in der Bezahlversion auch die Dateinamen. Bei der kostenfreien Classic-Version gibt es auch die Beschränkung auf nur ein verschlüsseltes Laufwerk, allerdings können Sie mehr als nur zwei Geräte verwenden.

Boxcryptor arbeitet mit nahezu allen bekannten Cloudspeichern zusammen.

Boxcryptor verwendet zur Verschlüsselung die als sicher eingestuften Verfahren AES (256 Bit) und RSA, ebenso wie bei SafeMonk verbleibt der Schlüssel ausschließlich beim Nutzer, sodass weder Boxcryptor selbst noch der Cloudspeicherdienst die Daten entschlüsseln kann. Die Software gibt es für Windows und Mac OS X sowie für alle wichtigen Mobilplattformen, wobei auch Windows Phone und BlackBerry unterstützt werden, und es wird ein Plug-in für den Chrome-Browser angeboten.

WAS SOLLTE VERSCHLÜSSELT WERDEN UND WAS NICHT?

Bevor es an das Verschlüsseln geht, sollten Sie sich überlegen, welche Daten überhaupt verschlüsselt werden sollen. Bei unverdächtigen Dateien, etwa Ihrer MP3-Musiksammlung oder auch Fotos, die Sie vielleicht ohnehin auf sozialen Netzwerken veröffentlichen oder mit Freuden teilen wollen, ist eine Verschlüsselung unnötig und erschwert das Teilen. Hier können Sie auf eine zusätzliche Verschlüsselung verzichten. Anders sieht die Lage dagegen bei persönlichen Dokumenten aus. Schriftstücke, Dokumente oder Geschäftsunterlagen, die Sie nicht in der Öffentlichkeit herumzeigen würden, sollten Sie auch in der Cloud schützen und nur in zuverlässig verschlüsselter Form übertragen und speichern.

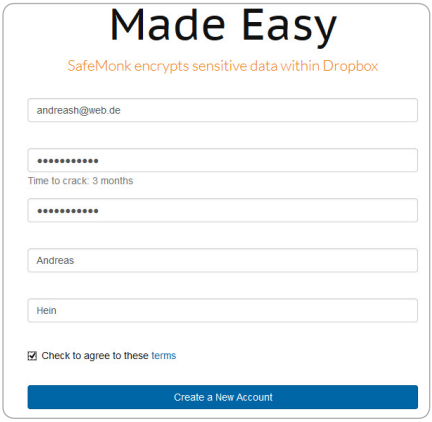
Die folgende Tabelle fasst die wichtigsten Merkmale der vorgestellten Verschlüsselungslösungen zusammen.

PRODUKT	EIGENSCHAFTEN	INTERNET
TrueCrypt	Relativ einfache Verschlüsselung von Dateien, aber keine Anbindung an Cloudspeicher. Nur für Desktopsysteme.	keine aktuelle Website mehr, Download z. B. über Websites von Computermagazinen
7-Zip	Sehr einfache und sichere Verschlüsselung einzelner Dateien, aber keine Anbindung an Cloudspeicher. Nur für Windows.	*www.7-zip.de*
SafeMonk	Sehr einfache und sichere Verschlüsselung, allerdings ausschließlich mit Dropbox. Für Windows, Mac OS, iOS und Android.	*www.safemonk.com*
Boxcryptor	Einfache Verschlüsselung mit nahezu allen Clouddiensten. Für alle üblichen Desktop- und Mobilplattformen nutzbar.	*www.boxcryptor.com*

Beispiel: Dateien verschlüsseln mit SafeMonk

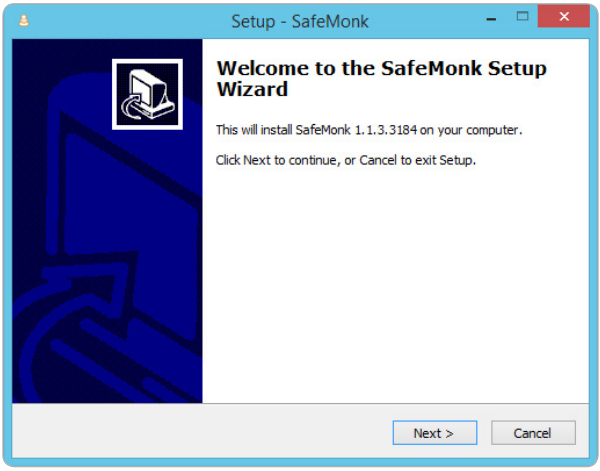
Wenn Sie bereits ein Konto bei Dropbox haben, können Sie mit SafeMonk sehr einfach Ihre Daten sicher verschlüsselt ablegen.

1. Als Erstes müssen Sie bei SafeMonk ein Konto einrichten. Dazu geben Sie Ihre E-Mail-Adresse in das Formular auf der Homepage (*www.safemonk.com*) ein. Danach legen Sie das Passwort fest, das für die Sicherheit ganz entscheidend ist. Als Qualitätsindikator wird Ihnen dabei angezeigt, wie lange es dauern würde, dieses Passwort zu knacken. Sie sollten ein ausreichend sicheres Passwort wählen. Schließlich tragen Sie Ihren Namen ein und akzeptieren die Nutzungsbedingungen. Über *Create a New Account* wird das Konto angelegt.



Die Anmeldung bei SafeMonk ist schnell vorgenommen.

2. Sie erhalten kurze Zeit später eine E-Mail an die angegebene Adresse. Klicken Sie dort auf den Bestätigungslink.
3. Danach laden Sie die Software herunter. Zunächst benötigen Sie auf Ihrem Desktop oder Notebook die SafeMonk-Software, um damit Ihr Konto einzurichten. Klicken Sie also auf der SafeMonk-Website auf *Downloads* und laden Sie die Software herunter.
4. Nach erfolgreichem Download installieren Sie die Software und melden sich mit Ihren Kontodaten an.

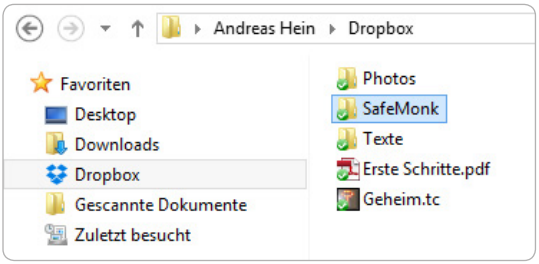


Installieren Sie auf Ihrem Rechner die SafeMonk-Software.

❺ Zum Abschluss wird Ihnen der Recovery Code angezeigt, der als Notoption zum Wiederherstellen der verschlüsselten Daten genutzt werden kann. Diesen Schlüssel sollten Sie notieren und an einem sicheren Ort aufbewahren.

Melden Sie sich beim Dienst mit Ihren Zugangsdaten an.

❻ Nun ist SafeMonk auch schon einsatzbereit. Nach erfolgreicher Installation erscheint in Ihrem Dropbox-Ordner ein Ordner namens *SafeMonk*.



In Ihrem *Dropbox*-Ordner ist der Ordner *SafeMonk* für die verschlüsselten Dateien eingerichtet.

❼ Alle Dokumente, die Sie in diesen Ordner verschieben, werden automatisch verschlüsselt und dann auf den Cloudserver übertragen. Sie können einzelne Dateien, aber auch ganze Ordner hierhin verschieben. Auf Ihrem Rechner werden Ihnen die Daten wie gewohnt angezeigt, solange Sie mit Ihrem SafeMonk-Konto angemeldet sind.

Die verschlüsselten Daten können Sie nach wie vor auch für andere Nutzer freigeben, allerdings müssen diese dazu ebenfalls über ein SafeMonk-Konto verfügen. Zur Nutzung des SafeMonk-Kontos auf Mobilgeräten (iOS und Android) können Sie eine App herunterladen.

8 DATENSICHERHEIT IN SOZIALEN NETZWERKEN

Noch mehr als Clouddienste haben in den letzten Jahren soziale Netzwerke die Internetnutzung revolutioniert. Seit Dienste wie Facebook, Twitter und Instagram ihren unaufhaltsamen Siegeszug angetreten haben, kennen viele Menschen kein Halten mehr, wenn es darum geht, auf die Schnelle ihre Meinungen, Kommentare und Fotos zu veröffentlichen. Doch nicht immer sind sie sich der Folgen ihres Tuns bewusst, denn einmal in der Öffentlichkeit der sozialen Netze präsentiert, lassen sich Inhalte nicht einfach wieder entfernen, selbst wenn man das möchte. Wenn Sie mit persönlichen Informationen nicht allzu freigiebig sein möchten, müssen Sie auf Facebook & Co. zwar nicht komplett verzichten, sollten aber einiges bei der Nutzung beachten.

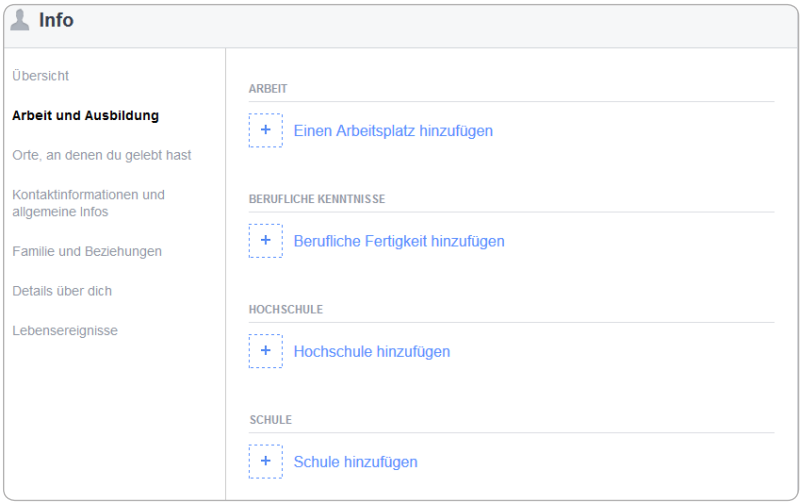
8.1 Wer sollte was wissen dürfen?

Ohne ständigen Zugriff auf soziale Netzwerke scheinen viele Mitmenschen kaum noch leben zu können. Neuigkeiten werden mit der immer größer werdenden Schar von »Freunden« ausgetauscht und kommentiert, man trifft sich auf Twitter und lästert hier über den gerade laufenden Fernsehkrimi ab, äußert seine Betroffenheit über die Naturkatastrophe am anderen Ende der Welt oder verabredet sich zwecks gemeinsamer Freizeitgestaltung.

Schon bei der Anmeldung geben bei den meisten Diensten die Nutzer viel von sich preis, wenn sie neben ihrem Namen und den Kontaktdaten noch Informationen zu schulischem und beruflichem Werdegang in ihre Profile eintragen, ihre Hobbys und Lieblingsbücher bzw. Filme benennen und ähnliche Angaben machen. Einerseits stellen diese Informationen die Grundlage der sozialen Netzwerke dar, denn man will ja schließlich mit alten oder neuen Freunden und Bekannten in Kontakt treten, andererseits veröffentlicht man damit auch Informationen, die man im realen Leben aus gutem Grund längst nicht jedem Unbekannten einfach so mitteilen würde.

Auch bei der alltäglichen Nutzung der Dienste kann es leicht problematisch werden. Unter Umständen lässt man sich aus einer Laune heraus zu einem missverständlichen Kommentar hinreißen oder verfasst eine Mitteilung, die man mit etwas Abstand im Nachhinein bereut. Zwar können Sie Bilder, Postings und Kommentare nachträglich wieder löschen, doch wenn sie bereits für Aufsehen gesorgt haben und im Freundeskreis oder gar darüber hinaus diskutiert werden, lässt sich die Tatsache, dass diese Meldungen einmal online waren, nicht mehr leugnen. Denn Bilder und Meldungen können jederzeit einfach

kopiert werden und sind damit auch nach dem Löschen des Originalbeitrags weiter verfügbar. Dass die Redewendung vom Internet, das nichts vergisst, durchaus keine weltfremde Floskel, sondern bittere Realität ist, haben schon viele Nutzer erfahren müssen.



Soziale Netzwerke sind an Informationen aus allen Lebensbereichen interessiert.

AUCH PERSONALABTEILUNGEN KENNEN FACEBOOK

Wenn Sie sich auf Facebook oder anderen sozialen Netzwerken öffentlich in Szene setzen, müssen Sie bedenken, dass diese Informationen auch Personen zugänglich sind, an die Sie zunächst gar nicht denken. So informieren sich immer öfter auch potenzielle Arbeitgeber über Stellenbewerber via Facebook, und nicht immer fällt das Fazit nach der Betrachtung der Chroniken positiv aus.

Nicht nur bei Bewerbungen können Facebook-Aktivitäten Folgen haben, auch in anderen Situationen werden die öffentlich zugänglichen Informationen vielleicht zu einem Nachteil:

- Arbeitnehmer können eine Abmahnung erhalten, wenn sie sich negativ über ihren Arbeitgeber geäußert haben.
- Schüler müssen mit Konsequenzen rechnen, wenn sie sich beleidigend über Lehrer oder Mitschüler äußern.
- Vermieter können eine Facebook-Recherche nutzen, um Mieter mit unerwünschten Eigenschaften und Aktivitäten zu identifizieren.
- Versicherungen können anhand der angegebenen Hobbys Kunden mit besonderen Risiken identifizieren und Angebote einschränken oder höhere Tarife fordern.
- Letztlich können auch Onlinebetrüger über das Sammeln persönlicher Daten in den Netzwerken Informationen gewinnen, die sie anschließend für das Social Engineering einsetzen, um maßgeschneiderte Phishing-Angriffe zu starten.

Bei der Nutzung sozialer Netzwerke gibt es zwei Aspekte im Hinblick auf Datenschutz. Zum einen geht es wie in den eben beschriebenen Fällen um die Daten, die Sie freiwillig veröffentlichen, und darum, wie diese von anderen Nutzern wahrgenommen werden oder was andere Nutzer mit diesen Informationen anfangen. Der andere Aspekt ist die Datensammlung der sozialen Netzwerke selbst. Diese erfassen Ihre Aktivitäten genau und nutzen diese Daten für eigene Zwecke. Da die meisten sozialen Netzwerke kostenfrei nutzbar sind und das nach eigenem Bekunden auch so bleiben soll, müssen sie sich ja auf andere Weise finanzieren. Die wichtigste Einnahmequelle ist die Werbung, und für Werbetreibende ist es wiederum sehr wichtig, dass ihre Werbemittel möglichst ohne Streuungsverluste genau bei der Zielgruppe ankommen. Je besser ein soziales Netzwerk Sie kennt und über Ihre Vorlieben und Gewohnheiten Bescheid weiß, desto wertvoller sind Sie für den Betreiber, denn diese Informationen kann es an die Werbetreibenden weiterverkaufen.

Grundlegende Regeln für den Umgang mit sozialen Netzwerken

Die Nutzung sozialer Netzwerke setzt natürlich voraus, dass Sie bereit sind, Informationen über sich bereitzustellen, und über Ihre Profile und Kontaktdaten für andere erreichbar und auffindbar sind. Dennoch sollten Sie nicht zu freigiebig sein und das Prinzip der Datensparsamkeit anwenden, also immer nur so viele Daten preisgeben, wie wirklich benötigt werden.

ECHTER NAME ODER PSEUDONYM?

Die Frage der Datensparsamkeit betrifft auch die grundlegende Entscheidung, ob Sie ein Konto in einem sozialen Netzwerk unter Ihrem richtigen Namen eröffnen möchten oder ob der Auftritt unter einem Pseudonym oder Spitznamen erfolgen soll. Prinzipiell sieht der Gesetzgeber im Telemediengesetz vor, dass eine Nutzung auch unter Pseudonym möglich sein soll, allerdings verlangt Facebook die Verwendung des echten Namens und behält sich bei Verstößen gegen diese Vorgabe vor, das Konto zu sperren. Rechtlich gibt es hier noch Klärungsbedarf, und es bleibt abzuwarten, wie über derartige Streitfälle entschieden wird.

Bei zweckgebundenen sozialen Netzwerken, etwa einem primär für berufliche Zwecke genutzten Netz wie etwa Xing, ergibt es keinen Sinn, ein Profil unter einem Pseudonym einzurichten, hier ist die Verwendung des echten Namens angeraten.

Bei der Anmeldung bei einem sozialen Netzwerk werden Sie zu einer möglichst umfassenden Angabe von Profildaten aufgefordert. Hierzu gehören auch Angaben zu Schulausbildung, Religionszugehörigkeit, politischen Ansichten, Familienstand und vielem mehr. Sie sollten sich immer genau überlegen, welche Informationen Sie mitteilen wollen und welche davon allen anderen Nutzern des Netzwerks angezeigt werden sollen. Mitunter ist es möglich, bestimmte Inhalte allgemein freizugeben und andere Profildaten dagegen nur ausgewählten Nutzern zugänglich zu machen.

Religiöse und politische Ansichten sollten Sie eher nicht veröffentlichen.

Die meisten sozialen Netzwerke ermöglichen es, verschiedenen Nutzergruppen unterschiedlichen Zugriff auf die eigenen Daten einzuräumen. Mitunter wird dabei nur zwischen allen Nutzern des Diensts (bzw. sogar allen Internetnutzern) und der Gruppe der Freunde unterschieden. Häufig gibt es auch

weitere Unterteilungen, etwa in Familie oder enge Freunde. Vor allem bei den Einstellungen zur Freigabe von Daten für die Gesamtheit der Nutzer sollten Sie nach Möglichkeit restriktiv vorgehen und nur die notwendigsten Angaben allgemein zugänglich machen.

WEITERE KONTAKTDATEN BESSER NICHT ANGEBEN

Abzuraten ist von der Weitergabe zusätzlicher Kontaktdaten. Soziale Netzwerke ermöglichen bereits die Erreichbarkeit über die interne Kommunikationsplattform und/oder die E-Mail-Adresse. Postanschrift und Telefonnummer sollten Sie nach Möglichkeit nicht mitteilen.

Auch die Veröffentlichung Ihrer Freundesliste können Sie bei vielen sozialen Netzwerken beschränken. Das kann durchaus sinnvoll sein, denn allein schon aus diesen Kontakten können andere Rückschlüsse auf Ihre Person ziehen.

SPERREN SIE SUCHMASCHINEN AUS

Kontrollieren Sie, ob das soziale Netzwerk die von Ihnen angegebenen persönlichen Daten nur anderen Nutzern des Netzwerks anzeigt oder ob diese Angaben auch Suchmaschinen zugänglich gemacht werden. Bei einigen sozialen Netzwerken können Sie in den Einstellungen festlegen, dass die eigenen Daten für Suchhilfen nicht zugänglich gemacht werden sollen.

In vielen sozialen Netzwerken gibt es Anwendungen von Drittanbietern, mit denen zusätzliche Funktionen nutzbar sind. Oftmals wollen diese Anwendungen auf Ihre Profildaten zugreifen, wobei die Informationen aus diesen Zugriffen häufig auch für unerwünschte Zwecke wie Werbung genutzt werden. Sie sollten daher bei Verwendung derartiger Anwendungen genau darauf achten, ob diese einen Zugriff auf die Profildaten verlangen, und sich genau überlegen, ob Sie das tatsächlich auch zulassen wollen.

8.2 Datenschutz- und Sicherheitseinstellungen bei Facebook

Das mit weitem Abstand meistgenutzte soziale Netzwerk ist nach wie vor Facebook. Auch wenn Angebote wie Twitter oder Instagram in letzter Zeit deutlich an Popularität zugelegt haben, bleiben sie im Hinblick auf die Nutzerzahlen immer noch deutlich hinter dem Marktführer zurück und sind auch im Hinblick auf Funktionsumfang und Nutzungszweck deutlich eingeschränkter als Facebook. Die auf berufliche Nutzung ausgerichteten Netzwerke wie Xing oder LinkedIn können es mit den Nutzerzahlen bei Facebook ebenfalls bei Weitem nicht aufnehmen. Wir zeigen daher speziell für Facebook, wie Sie ganz konkret Datenschutzeinstellungen anpassen können.

Facebook-Datenschutz als Dauerthema

Gerade Facebook steht im Hinblick auf den Datenschutz immer wieder im Fokus der Datenschützer. Zum einen gibt es grundsätzliche Kritik an einigen Praktiken, zum anderen sorgen die zahlreichen Änderungen und Neuregelungen der Datenschutzbestimmungen für einigen Zündstoff, denn in der Regel können Nutzer den geänderten Bestimmungen nur zustimmen oder müssen andernfalls ihr Konto aufgeben.

Zuletzt hatte das Unternehmen Anfang 2015 bei vielen Datenschützern und Nutzern für Unmut gesorgt, als es wieder einmal die Nutzungsbedingungen geändert hatte. Dabei hatte es sich das Recht einräumen lassen, das Surfverhalten der Nutzer auch außerhalb von Facebook über Cookies zu erfassen, um anhand der gewonnenen Daten personalisierte Werbebanner einblenden zu können. Zuvor waren primär nur solche Aktionen ausgewertet worden, die im direkten Zusammenhang mit der Facebook-Nutzung stehen, also etwa das Anklicken der Gefällt-mir-Buttons.

Im Gegenzug verspricht Facebook nun, die Werbeannoncen besser zu erklären, indem Nutzer eine Schaltfläche anklicken können, über die eine Begründung dafür angezeigt wird, dass gerade diese Werbung erscheint. Außerdem können Nutzer unpassende Werbung kennzeichnen und bekommen in der Folge von diesem Anbieter keine weiteren Werbebanner mehr angezeigt.

Facebook erklärt Ihnen, warum Sie eine bestimmte Werbung zu sehen bekommen.

Ebenso will sich Facebook eine Zugriffsoption auf die aktuellen Standortdaten der Nutzer einräumen lassen, um hierüber ortsbezogene Dienste anbieten zu können. Wenn Sie sich also als Fan der italienischen Küche zu erkennen gegeben haben, könnte sich Facebook künftig bei Ihnen melden, wenn Sie in einer fremden Stadt gerade in der Nähe einer Pizzeria sind, und Sie auf das aktuelle Tagesgericht aufmerksam machen.

WIDERSPRUCH IST ZWECKLOS

Eine Widerspruchsmöglichkeit gegen die neuen Bestimmungen gibt Facebook nicht, was europäische Datenschützer für gesetzwidrig halten. Die von einigen Facebook-Nutzern in ihre Timeline eingebauten Widerspruchserklärungen haben jedenfalls keine Wirkung. Wer sich auf die geänderten Bestimmungen nicht einlassen will, hat nur die Option, das Facebook-Konto zu löschen. Dies dürfte aber für die wenigsten Nutzer tatsächlich infrage kommen.

PROFILINFORMATIONEN AUF DAS NOTWENDIGSTE BESCHRÄNKEN

Facebook möchte von seinen Nutzern jede Menge persönlicher Daten sammeln und fragt daher für das Profil nach zahllosen Informationen. Sie sollten bei der Anmeldung zunächst nur die wirklich notwendigsten angeben und im Zweifelsfall Einträge offen lassen. Wenn Ihnen für die Nutzung bestimmte Angaben später doch sinnvoll und wichtig erscheinen, können Sie Ihre Auskünfte jederzeit ergänzen. Dazu wählen Sie auf Ihrer Startseite einfach den Bereich *Info* aus.

Sicherheitsrelevante Einstellungen

Facebook ermöglicht es, eine Art Zwei-Faktor-Authentifizierung durchzuführen. Anders als bei anderen Diensten ist die zusätzliche Authentifizierung jedoch nicht bei jeder Anmeldung vorgesehen, sondern nur dann, wenn Sie das erste Mal von einem neuen Gerät oder einer neuen Software aus auf Ihr Facebook-Konto zugreifen wollen. In diesem Fall können Sie in den Sicherheitseinstellungen vorgeben, dass ein Sicherheitscode eingegeben werden muss, den Sie auf Ihr Smartphone geschickt bekommen. Wenn Sie diesen Zusatzschutz aktiviert haben, kann sich ein Datendieb, der Ihr Passwort ausspioniert hat, damit nicht mehr direkt von einem fremden Rechner aus an Ihrem Konto anmelden.

Über den an Ihr Handy geschickten Code können Sie Ihr Facebook-Konto sicherer machen.

Sie können sich auch Warnungen per SMS oder E-Mail zusenden lassen, wenn von einem neuen Gerät aus ein Anmeldeversuch unternommen wird. Ebenso können Sie sich eine Übersicht über die Browser und Geräte anzeigen lassen, mit denen Sie Facebook verwenden, und von wo aus Sie sich gerade bei Facebook angemeldet haben.

Sollten Sie einmal Ihr Passwort vergessen haben, bekommen Sie mit *Zuverlässige Kontakte* wieder eine Zugangsmöglichkeit. Dazu wählen Sie drei bis fünf Ihrer Facebook-Freunde aus. Diesen wird im Notfall ein Teil eines Sicherheitscodes von Facebook zugesendet, den sie Ihnen anschließend mitteilen können. Mit dem zusammengesetzten Code können Sie danach wieder auf Ihr Facebook-Konto zugreifen.

Verschiedene Sicherheitsmaßnahmen dienen dem Schutz Ihres Facebook-Kontos.

Zu diesen Einstellungsoptionen gelangen Sie über das Facebook-Menü *Einstellungen* und den Punkt *Sicherheit*. Das Einstellungsmenü rufen Sie über das Dreieck in der Facebook-Titelzeile auf.

FACEBOOK-KONTO DEAKTIVIEREN UND LÖSCHEN

Auf der Einstellungsseite können Sie Ihr Facebook-Konto auch deaktivieren. Dabei haben Sie die Möglichkeit, das Konto entweder komplett zu löschen oder zunächst nur auf Zeit auszusteigen und den Account für eine Zeitspanne zwischen einem Tag und vier Wochen temporär stillzulegen. Auch wenn Sie das Konto komplett deaktivieren wollen, haben Sie eine Schonfrist von 14 Tagen. Loggen Sie sich in dieser Zeit erneut auf Facebook ein, wird Ihr Konto wieder aktiviert. Nach dem Löschen des Kontos dauert es einige Wochen, bis Facebook alle von Ihnen hochgeladenen Daten entfernt hat. Vor dem Löschen können Sie Kopien dieser Daten, etwa Fotos oder Videos, über die *Allgemeinen Einstellungen* noch herunterladen.

Datenschutzeinstellungen

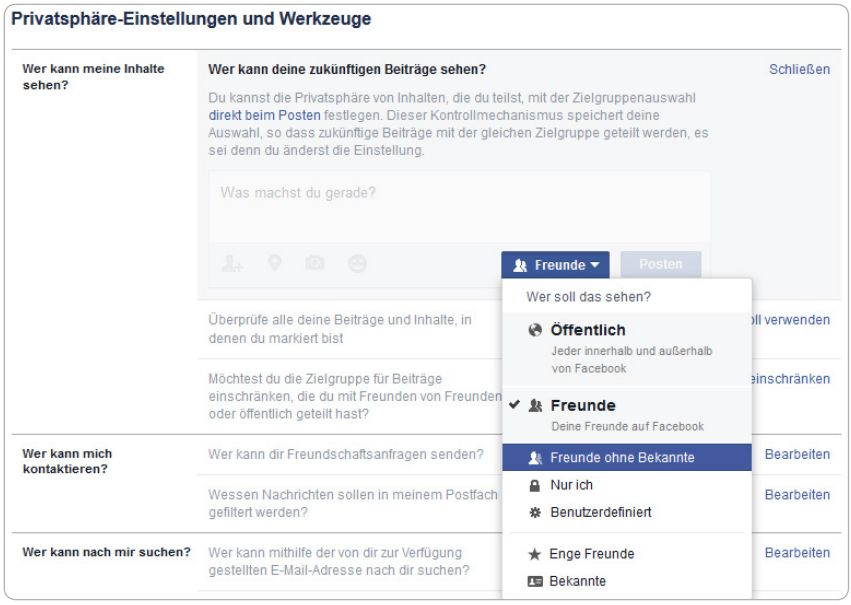
Es gibt in Facebook zahlreiche Einstellungsoptionen mit Relevanz für den Schutz der online gestellten Daten. Sie können etwa beeinflussen, für wen Sie überhaupt erreichbar sein wollen oder welcher Personenkreis welche Inhalte zu sehen bekommt.

Die datenschutzrelevanten Einstellungen sind auf verschiedene Bereiche verteilt. Bereits im Bereich *Allgemein* können Sie einige Anpassungen vornehmen. Hier könnten Sie den Namen ändern, wenn Sie nicht mehr mit Ihrem richtigen Namen, sondern unter einem Pseudonym in Facebook auftreten wollen. Allerdings verlangt Facebook die Verwendung des Klarnamens und behält sich vor, gegen Verstöße vorzugehen.

Wenn Sie auf Facebook nicht für jedermann auffindbar sein wollen, kann es angeraten sein, nicht Ihre allgemein bekannte E-Mail-Adresse zu verwenden, über die Sie auch für Dritte eindeutig identifiziert werden können. Weichen Sie bei Bedarf auf eine eigens für die Facebook-Nutzung angelegte Mailadresse aus und tragen Sie diese Adresse als primäre E-Mail-Adresse ein.

Sie können eine ausschließlich für Facebook angelegte E-Mail-Adresse verwenden.

Die meisten Einstellungen mit Relevanz für den Datenschutz nehmen Sie in der Rubrik *Privatsphäre* vor. Hier haben Sie unter *Wer kann meine Inhalte sehen?* als Erstes die Möglichkeit, festzulegen, welche Standardeinstellung für die Sichtbarkeit neuer Beiträge Sie nutzen möchten. Prinzipiell können Sie bei jedem neuen Posting festlegen, welche Nutzergruppe diesen Beitrag sehen kann. Treffen Sie keine explizite Wahl, wird eben dieser Standardeintrag genommen. Es stehen zunächst die Gruppen *Freunde* und *Öffentlich* zur Auswahl,



Sie können die Standardeinstellung zur Sichtbarkeit Ihrer Beiträge ändern.

darüber hinaus finden Sie in *Weitere Optionen* eine Beschränkung auf *Nur ich*, wenn Sie die Mitteilungen ausschließlich für sich selbst anlegen wollen, oder eine Beschränkung auf bestimmte *Listen*.

Solche Listen können etwa *Enge Freunde* oder *Familie* sein, die Facebook schon vorgegeben hat, Sie können aber auch eigene Listen anlegen. Wie bereits gesagt, ändern Sie hier lediglich die Standardeinstellung, bei jedem Posting können Sie direkt immer auch eine andere Zielgruppe auswählen. Zudem haben Sie die Möglichkeit, die Sichtbarkeit älterer Beiträge nachträglich einzuschränken und sich Beiträge und Inhalte anzeigen zu lassen, in denen Sie markiert wurden.

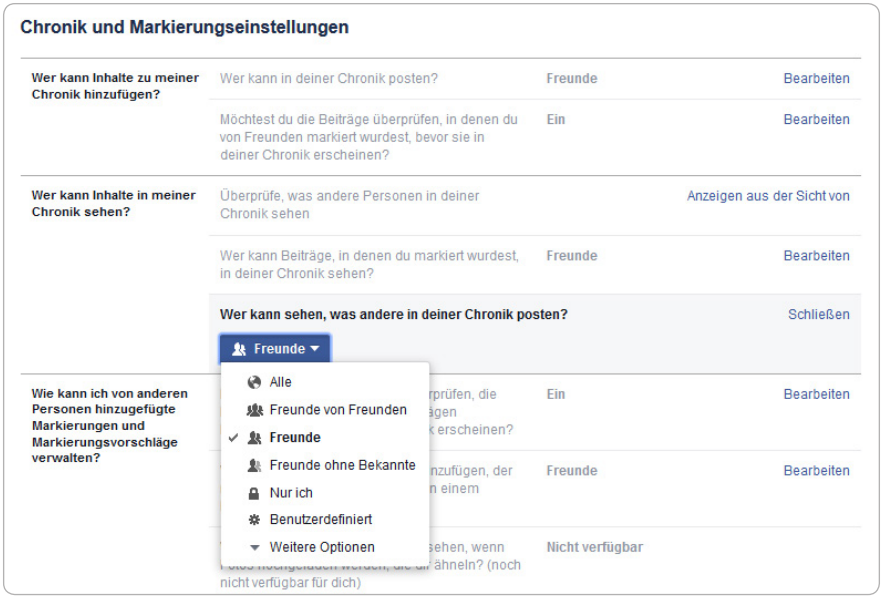
Im nächsten Abschnitt (*Wer kann mich kontaktieren?*) legen Sie fest, wer Sie über Facebook kontaktieren oder eine Freundschaftsanfrage senden darf. Sie haben die Auswahl zwischen sämtlichen Facebook-Nutzern (*Alle*) und *Freunde von Freunden*, wobei diese pauschale Beschränkung in den meisten Fällen keinen wirklichen Sinn hat, wenn man tatsächlich in einem sozialen Netzwerk aktiv sein will.

Beschränkungen hinsichtlich der eigenen Auffindbarkeit können Sie dagegen besser im Punkt *Wer kann nach mir suchen?* vornehmen. Hier haben Sie die Möglichkeit, festzulegen, ob alle Facebook-Nutzer Sie über Ihre E-Mail-Adresse finden dürfen oder dies auf Freunde bzw. Freunde von Freunden beschränkt bleiben soll. Gleiches gilt für die Telefonnummer, sofern Sie sie bei Facebook angegeben haben. Wenn Sie bei Facebook ohnehin schon eine E-Mail-Adresse hinterlegt haben, die eigens dafür eingerichtet wurde und die Sie ansonsten nicht nutzen, brauchen Sie hier keine weitere Einschränkung vorzunehmen. Verwenden Sie dagegen eine allgemein bekannte E-Mail-Adresse und möchten die Kontaktaufnahme beschränken, wählen Sie die Option *Freunde*.

Legen Sie fest, ob alle Facebook-Nutzer Sie über Ihre E-Mail-Adresse finden sollen oder nicht.

Schließlich können Sie noch festlegen, ob *Suchmaschinen* Zugriff auf Ihre Chronik in Facebook erhalten und die Inhalte verlinken können sollen. Wenn Ihnen das zu viel Öffentlichkeit ist, können Sie den direkten Zugriff der Suchmaschinen hier verhindern.

Datenschutzrelevante Einstellungen sind auch im Bereich *Chronik und Markierungseinstellungen* zu finden. So legen Sie hier fest, wer auf Ihrer Chronik Inhalte hinzufügen darf. Sie können dies für alle Freunde zulassen oder Ihre Chronik ausschließlich mit eigenen Postings füllen. Ebenso haben Sie die Möglichkeit, sich Ihre Chronik einmal aus der Perspektive anderer Nutzer anzusehen und festzulegen, wer sehen kann, was andere in Ihrer Chronik gepostet haben.



Auch im Bereich *Chronik und Markierungseinstellungen* gibt es datenschutzrelevante Einstellungsoptionen.

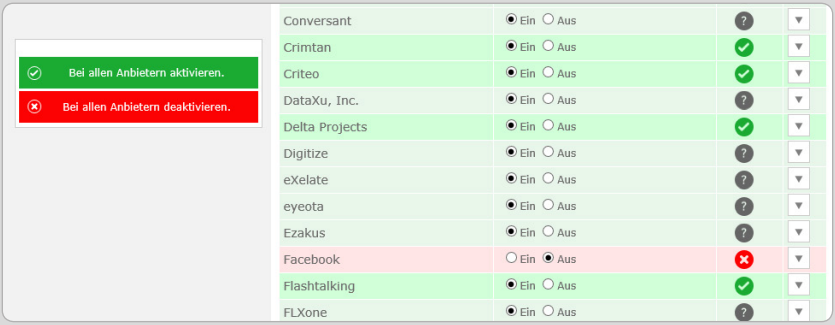
Im Bereich *Blockieren* können Sie eine Liste mit Facebook-Kontakten anlegen, mit denen Sie nicht wirklich viele Inhalte teilen möchten. Wer auf der Liste *Eingeschränkt* steht, bekommt ausschließlich Inhalte und Beiträge angezeigt, die Sie ohnehin als *Öffentlich* gekennzeichnet haben und die daher jeder andere Facebook-Anwender ebenfalls lesen kann. Die Person, die Sie auf diese Liste

setzen, bekommt von diesem Vorgang nichts mit. Dies gilt im Übrigen auch für andere Listen, die Sie verwenden oder selbst anlegen. Die Kontakte, die Sie in diese Listen einsortieren, erhalten darüber keine Informationen.

Von Bedeutung für Ihre Privatsphäre sind schließlich noch die Einstellungsoptionen im Bereich *Werbeanzeigen*. Hier können Sie beispielsweise schon einmal vorab einer Werbung mit Ihrem Namen oder unter Verwendung Ihrer Bilder widersprechen, falls Facebook diese Option künftig einmal nutzen wird. Auch die Weiterverwendung der von Ihnen ausgesprochenen Empfehlungen, die Sie durch das Anklicken des Gefällt-mir-Buttons vorgenommen haben, können Sie hier einschränken. Wählen Sie bei den beiden Optionen *Niemand* aus, um die Datenweitergabe auf ein Minimum zu reduzieren.

PERSONALISIERTE WERBUNG VERHINDERN

Hier wird Ihnen beschrieben, wie Sie die Auswertung Ihres Surfverhaltens außerhalb von Facebook zur Optimierung der Werbeanzeigen blockieren können. Dazu können Sie auf einer externen Website einer europäischen Werbe-Allianz eine Einstellung vornehmen, die per Cookie auf Ihrem Rechner gespeichert wird. Hiermit können Sie allerdings nur die Einblendung personalisierter Werbebanner verhindern, die Sammlung der Daten unterbinden Sie so nicht. Damit die Abbestellung funktioniert, müssen die Cookies der Werbe-Allianz dauerhaft gespeichert werden. Nutzen Sie auf Ihrem Rechner eine Cookie-Lösung, bei der nur temporäre Cookies erlaubt sind, nutzt diese Option nichts. Ebenso gibt es Probleme, wenn Sie in Ihrem Browser Cookies von Drittanbietern generell verboten haben. Die Website der European Digital Advertising Alliance erreichen Sie unter *www.youronlinechoices.com/de/praferenzmanagement/*.



Sie können Facebook signalisieren, dass Sie keine personalisierte Werbung wünschen.

Gruppen und Listen verwenden

Auf Facebook sind Sie natürlich in erster Linie selbst verantwortlich, wenn es um die Frage geht, welche Informationen Sie veröffentlichen und vor allem auch wem Sie diese Informationen zugänglich machen wollen. Die Freigabe sämtlicher Postings an alle Freunde oder gar an die Öffentlichkeit ist sicher nicht empfehlenswert, da Ihre Beziehungen zu den Facebook-Freunden unterschiedlicher Natur sind. Und einem eher flüchtigen Bekannten werden Sie im echten Leben ja auch nicht dieselben Informationen geben wie einem engen Freund oder Familienangehörigen, und mit Ihrem Chef werden Sie andere Informationen teilen wollen als mit einem Kollegen.

Bei Facebook sollten Sie daher darauf achten, wer Ihre Postings zu Gesicht bekommt, und immer im Einzelfall entscheiden, wer die angemessene Zielgruppe ist. Vor jedem Posting können Sie die Zielgruppe bestimmen. Eine wesentliche Differenzierungsmöglichkeit bieten die bereits erwähnten Listen. Diese Listen werden von Facebook selbst als sogenannte intelligente Listen erstellt, wobei etwa Freunde mit übereinstimmenden Profilmerkmalen in einer solchen Liste (z. B. Freunde, die dieselbe Schule wie Sie besucht haben, Freunde aus Ihrem Wohnort etc.) zusammengefasst werden. Sie können aber auch weitere individuelle Listen erstellen und selbst aussuchen, welche Kontakte in die jeweilige Liste aufgenommen werden.

Machen Sie von der Möglichkeit zum Erstellen von Freundeslisten Gebrauch.

Eine weitere Option neben den Listen zur Differenzierung der Kontakte in Facebook sind die Gruppen. Neben öffentlichen Gruppen, zu denen jeder Interessent Zugang hat, gibt es auch private bzw. geheime Gruppen, die nur ausgewählte Teilnehmer nach einer Einladung zulassen. Die Einrichtung privater

Gruppen ist jedem Nutzer möglich, und die Inhalte, die in diesen geheimen Gruppen gepostet werden, können auch nur andere Mitglieder sehen. Ebenso können in den geheimen Gruppen ausschließlich die Mitglieder sehen, wer sonst noch dieser Gruppe angehört.

In Gruppen werden Nachrichten in einem geschlossenen Kreis ausgetauscht.

Letztlich sollten Sie bei allen Einschränkungen der Leserschaft Ihrer Facebook-Mitteilungen daran denken, dass die Inhalte auch einer breiteren Öffentlichkeit zugänglich gemacht werden können, wenn Mitglieder der Listen und Gruppen Postings weiterverbreiten.

9 VERSCHLÜSSELTER NACHRICHTENAUSTAUSCH

Schon im Kapitel zur sicheren Nutzung von Cloudspeicherdiensten haben wir darauf hingewiesen, dass der Verschlüsselung eine zentrale Rolle bei der sicheren Nutzung des Internets zukommt. Unverschlüsselte Datenübertragung ist leider immer noch bei den meisten Diensten und Kommunikationsangeboten der Standard, doch angesichts der allgegenwärtigen Überwachung sollte sich eigentlich jeder Anwender wehren und selbst verschlüsseln, was gar nicht so kompliziert und aufwendig ist.

9.1 Abhörsicheres Surfen im Web

Zur verschlüsselten Übertragung von Informationen im Web haben wir Ihnen bereits in den Kapiteln zum Onlinebanking und Onlineshopping sowie zu den allgemeinen Sicherheitshinweisen die wichtigsten Informationen gegeben.

Sie müssen darauf achten, dass im Browser eine abhörsichere Verbindung per SSL-/TLS-Verschlüsselung genutzt wird. Dies betrifft insbesondere Seiten, über die Sie sensible Daten übertragen. Das sind nicht nur Konto- und Kreditkartendaten sowie Anmeldedaten wie Passwörter, sondern alle Informationen, die Sie nicht unbedingt mit der Allgemeinheit teilen möchten.

AUCH APPS SOLLTEN MIT VERSCHLÜSSELUNG ARBEITEN

Bei Apps sollten Sie darauf achten, dass sie ebenfalls Verschlüsselung bieten. Greifen Sie ansonsten besser auf den Browser zurück, sofern Sie einen Dienst damit in verschlüsselter Form nutzen können. Besonders kritisch ist die unverschlüsselte Übertragung in öffentlichen WLANs, da es hier sehr einfach ist, unverschlüsselte Daten abzufangen und Informationen zu missbrauchen.

Bei besonders sensiblen Daten sollten Sie sich nicht nur auf die https-Anzeige im Browseradressfeld verlassen, sondern weitere Informationen zum Zertifikat einholen und diese auf ihre Konsistenz mit dem jeweiligen Angebot hin überprüfen.

9.2 Verschlüsselte Chat- und Messenger-Lösungen

Ein großer Teil der Internetkommunikation läuft über Chat- und Messenger-Lösungen in sozialen Netzwerken oder über eigenständige Lösungen. Die populärste Anwendung ist WhatsApp, das außer dem Austausch einfacher Textnachrichten auch die Übertragung von Bildern, Videos und Audiodateien ermöglicht. WhatsApp ist allerdings auf Mobilgeräte beschränkt, unterstützt aber alle relevanten Plattformen. Da für die Nachrichtenübertragung per WhatsApp bei Daten-Flatrates keine direkten Gebühren anfallen, hat das System einen enormen Erfolg, weil es die teuren SMS und MMS ersetzt. Ende 2014 sollen weltweit bereits über 700 Millionen aktive Nutzer bei WhatsApp registriert gewesen sein.

WhatsApp jetzt mit Verschlüsselung

Allerdings gab es schon frühzeitig erhebliche Kritik an WhatsApp, da das System in Hinblick auf den Datenschutz bedenklich war, weil Nachrichten völlig unverschlüsselt übertragen wurden. Hinsichtlich der Verschlüsselung ist diese pauschale Kritik seit Ende letzten Jahres nicht mehr gerechtfertigt. Seit November 2014 können Nutzer von Android-Geräten per WhatsApp verschlüsselt kommunizieren. Für iOS-Geräte wurde die Verschlüsselung im März 2015 ermöglicht, und andere Mobilplattformen sollen bald folgen.

WhatsApp, das seit einiger Zeit zu Facebook gehört, arbeitet mit einer von Sicherheitsexperten einhellig gelobten Lösung, die mit einer echten Ende-zu-Ende-Verschlüsselung arbeitet. Diese kam zuvor schon im Open-Source-Messenger TextSecure zum Einsatz und zeichnet sich nicht allein durch die Sicherheit aus – darüber hinaus ist einfach nutzbar und bürdet Anwendern keinerlei Aufgaben zur Schlüsselerstellung und Verteilung auf.

WhatsApp, der Marktführer unter den mobilen Messengern, bietet jetzt eine Verschlüsselung an.

Dennoch gibt es immer noch etliche Kritiker, die WhatsApp nicht über den Weg trauen, vor allem seit der Übernahme durch Facebook. Angesichts der wenig Vertrauen erweckenden Datenschutzpolitik von Facebook warnen sie vor dem Entstehen einer allzu übermächtigen Datenkrake, die riesige Informationsmengen zu einzelnen Nutzern anhäufen könnte, und raten daher von einer Nutzung ab.

Weitere verschlüsselte Messenger-Anwendungen

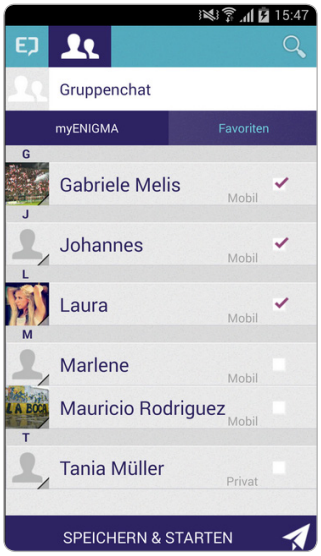
Schon lange bevor WhatsApp auf die Kritik reagierte und sich um eine Verschlüsselung bemühte, waren andere Dienste mit dem Versprechen einer abhörsicheren Kommunikation angetreten und konnten sich zunächst über schnell wachsende Nutzerzahlen freuen.

Zu den bekanntesten WhatsApp-Alternativen gehört Threema, das von einem Schweizer Unternehmen betrieben wird, dessen Server sich auch in der Schweiz befinden, sodass sich Geheimdienste wie die NSA oder der britische GCHQ nicht ganz so einfach Zugang zu den Servern verschaffen können.

Threema arbeitet ebenfalls mit einer Ende-zu-Ende-Verschlüsselung, sodass die Daten nicht auf den Servern, über die die Kommunikation läuft, abgehört werden können. Zwar macht Threema den Sourcecode der Verschlüsselungslösung nicht vollständig öffentlich, dennoch gibt es bei den meisten Experten keine Zweifel an der Zuverlässigkeit und Seriosität dieses Angebots.

Threema war einer der ersten Messenger mit einer sicheren Verschlüsselung.

Threema ermöglicht verschlüsselte Gruppen-Chats, und auch Fotos, Videos oder andere Daten werden ebenso zuverlässig verschlüsselt wie die Textnachrichten. Ebenso wie WhatsApp gibt es Threema bislang ausschließlich für Mobilplattformen, wobei neben Android und iOS seit Kurzem auch eine Version für Windows Phone angeboten wird. Bei den Nutzerzahlen kann Threema im Vergleich zu WhatsApp nicht mithalten. Ende 2014 sollen etwa 3,3 Millionen Nutzer bei dem Dienst registriert gewesen sein.



Verschlüsselte Gruppen-Chats sind mit myEnigma ebenfalls möglich.

Ein ebenfalls von einem Schweizer Unternehmen stammender verschlüsselnder Messaging-Dienst ist myEnigma. Dieses Angebot wird von Experten ebenfalls als sehr sicher eingestuft, da es eine Ende-zu-Ende-Verschlüsselung bietet. Zum Einsatz kommen hier symmetrische Schlüssel, was zwar einige Risiken birgt, im Gegenzug werden diese Schlüssel aber nach nur drei Tagen automatisch gewechselt. Selbst wenn es einem Angreifer mit hohem Aufwand gelingen sollte, einen Schlüssel zu knacken, könnte er damit nichts anfangen, da zwischenzeitlich wieder ein anderer Schlüssel verwendet wird. Der Dienst bietet zusätzlich auch eine Option für verschlüsselte Gruppen-Chats an.

Eine Besonderheit der myEnigma-App ist ein verschlüsselter SMS-Modus, über den Sie verschlüsselte Kurznachrichten auch bei Störungen des Internetzugangs versenden können oder in Gegenden, in denen gar keine mobile Internetverbindung vorhanden ist. Wie bei Threema lassen sich auch Bilder, Videos und Audiodateien verschlüsseln.

Die myEnigma-App gibt es in Versionen für iOS, Android und BlackBerry, für Windows Phone ist eine Version geplant. Die Nutzung ist kostenfrei möglich, allerdings soll es längerfristig eine Kostenbeteiligung der Nutzer geben.

Eine etwas andere Krypto-Messenger-Lösung als die bislang vorgestellten Systeme ist Wickr. Sie bietet ebenfalls eine Ende-zu-Ende-Verschlüsselung, die mit dem sicheren AES-Verfahren (256 Bit) arbeitet. Zusätzlich entfernt Wickr allerdings verräterische Metadaten der Dateien, wie etwa Ort oder Zeit der

Erstellung, oder Daten der genutzten Hardware. Eine andere Besonderheit ist die Option, verschlüsselte Nachrichten mit einem Verfallstermin zu versehen. Zum angegebenen Termin werden die Daten auf dem Empfängergerät automatisch gelöscht. Allerdings sollten Sie diese Funktion nicht überschätzen, denn wenn beispielsweise von einem Foto beim Empfänger bereits ein Screenshot erstellt wurde, hilft auch das Löschen des Originals nicht mehr.

Wickr bezeichnet sich selbst als Top-Secret-Messenger.

Wickr gibt es nicht nur als App für iOS und Android, sondern seit Ende 2014 auch als Desktopanwendung für Mac OS, Windows und Linux. Anders als bei den anderen Messenger-Lösungen können Sie hier also auch mit Gesprächspartnern kommunizieren, die nicht per Smartphone oder Tablet online sind, sondern ein Notebook verwenden oder am Desktoprechner arbeiten.

ÜBERSICHT ÜBER VERSCHLÜSSELTE MESSENGER-APPS

Es gibt viele weitere Messenger-Lösungen, die ebenfalls einen verschlüsselten Nachrichtenaustausch ermöglichen. Eine Übersicht zu den Sicherheitsfeatures der zahlreichen Systeme bietet eine Scorecard der Electronic Frontier Foundation, auf der Sie auf einen Blick erkennen können, welchen Sicherheitsanforderungen die Messenger genügen und welchen nicht. Dieses Angebot finden Sie unter *https://www.eff.org/de/secure-messaging-scorecard*.

MESSENGER MIT ENDE-ZU-ENDE-VERSCHLÜSSELUNG	PLATTFORMEN, BESONDERHEITEN	INTERNET
WhatsApp	Android, iOS, Windows Phone, BlackBerry, Nokia S40/S60, Verschlüsselung derzeit (Frühjahr 2015) noch nicht in allen Versionen implementiert	*www.whatsapp.com*
Threema	Android, iOS, Windows Phone	*www.threema.com*
myEnigma	Android, iOS, BlackBerry	*www.myenigma.com*
Wickr	Android, iOS, Windows, Mac OS X, Linux, Nachrichten auch mit Verfalls- bzw. Löschdatum möglich	*www.wickr.com*

9.3 Verschlüsselung für VoIP-Telefonate

Das Telefonieren via Internet (*Voice over Internet Protocol*, kurz auch VoIP) ist unaufhaltsam auf dem Vormarsch. In wenigen Jahren wird die VoIP-Technik auch an Festnetzanschlüssen die konventionelle Anschlusstechnik ersetzt haben, und alle Telefonate werden über das Internet geführt werden. Allerdings hat VoIP gegenüber dem klassischen Telefonnetz einen großen Nachteil: Genau wie bei den meisten Internetdiensten erfolgt auch bei VoIP die Übertragung unverschlüsselt und kann sehr einfach abgehört werden.

VoIP per App verschlüsseln

Allerdings gibt es für VoIP ein recht großes Angebot an Verschlüsselungslösungen. Im Vergleich zum Aufwand, der betrieben werden muss, um eine konventionelle Mobilfunkverbindung zu verschlüsseln, ist die VoIP-Verschlüsselung wesentlich einfacher und auch günstiger.

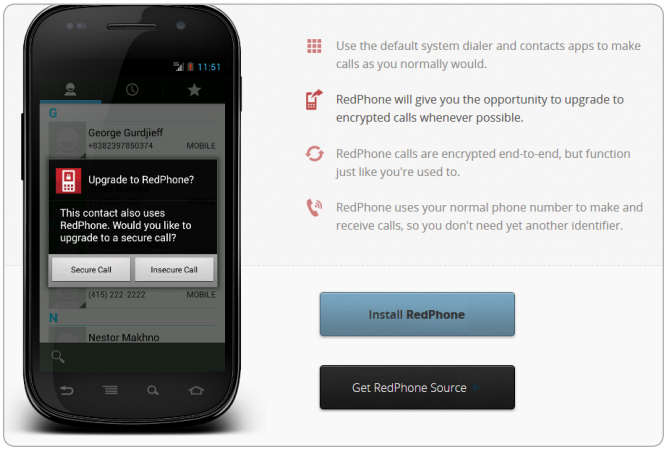
Auf Smartphones reicht eine einfache App, allerdings benötigen Sie ein Konto bei einem VoIP-Provider. Zu den bekanntesten Lösungen dieser Art gehört Linphone, das vor allem den Vorteil hat, dass es Apps und Anwendungen für alle wichtigen Plattformen gibt. Neben den Mobilplattformen iOS, Android und Windows Phone werden auch Mac OS X, Windows und sogar Linux unterstützt. Die Nutzung setzt lediglich die Installation der App sowie die Einrichtung eines VoIP-Kontos voraus. Die Verschlüsselung erfolgt über den VoIP-Standard ZRTP, der nach aktuellem Stand als sicher gilt.

Linphone gehört zu den beliebtesten VoIP-Clients und bietet eine sichere Verschlüsselung.

Wenn Sie VoIP-Telefonate über Ihren Mobilfunkanschluss führen wollen, müssen Sie allerdings abklären, ob in Ihrem Vertrag die VoIP-Nutzung erlaubt ist. Bei einigen Verträgen werden VoIP-Verbindungen blockiert, weil sich die Netzbetreiber das lukrative Geschäft mit den konventionellen Telefonaten im Mobilfunknetz nicht entgehen lassen wollen.

Eine etwas andere Möglichkeit zur verschlüsselten Kommunikation bieten die Apps RedPhone (für Android) und Signal (für iOS) des Herstellers Open Whisper Systems. Beide verwenden wie Linphone die ZRTP-Verschlüsselung, anders als bei Linphone ist für die Nutzung jedoch kein zusätzliches Konto bei einem VoIP-Provider notwendig. Nutzer müssen sich lediglich mit ihrer Telefonnummer registrieren, und auch zur Verbindungsaufnahme wird diese Rufnummer verwendet. Bislang gibt es die beiden ausschließlich für die beiden Plattformen iOS und Android, allerdings wollen die Hersteller demnächst auch Plug-ins für Browser anbieten.

Die Verbindungen zwischen den Teilnehmern laufen über die Server der Dienstanbieter, sodass von außen nicht einmal die Verbindungsdaten festgestellt werden können. Potenzielle Überwacher sehen lediglich, dass ein Anrufer eine Verbindung zu einem Signal- oder RedPhone-Server herstellt, nicht aber, mit wem er darüber tatsächlich telefoniert. Die Betreiber der Dienste versichern, dass sie keine Verbindungsdaten speichern, sodass auch keine Herausgabe dieser Informationen an Behörden möglich ist. Die Apps sind nicht nur für die verschlüsselte Sprachübertragung nutzbar, sondern auch als abhörsichere Messenger- und Chat-Tools.



Neben Signal für iOS gibt es mit RedPhone auch für Android eine verschlüsselungsfähige App.

Der eigene VoIP-Server

Für VoIP-Telefonate in geschlossenen Gruppen, also etwa innerhalb des Freundes- oder Familienkreises, benötigen Sie nicht zwangsläufig die Dienste eines VoIP-Anbieters. Vielmehr können Sie mit relativ einfachen Mitteln auch einen eigenen VoIP-Server betreiben, über den Sie mit den entsprechenden Clients vom Desktop oder Notebook aus per VoIP miteinander telefonieren können. Auch für die beiden wichtigsten Mobilplattformen iOS und Android sind Apps verfügbar.

Eine der bekannteren Lösungen, die auch im Privatbereich verbreitet ist, ist der Open-Source-Server Mumble bzw. Murmur, der mit Clients wie Mumble (iOS) oder Plumble (Android) zusammenarbeitet. Das System ist primär ein Sprachkonferenzsystem und kommt häufig als Kommunikationskanal bei Onlinespielen zum Einsatz, kann aber auch für eine verschlüsselte VoIP-Kommunikation verwendet werden. Einsatzvoraussetzung für den Server ist ein Breitbandinternetanschluss, der über eine Upload-Bandbreite von mindestens 256 MBit/s verfügen sollte, um eine akzeptable Sprachqualität zu ermöglichen, die allerdings bei den meisten DSL-Anschlüssen erreicht wird. Zudem benötigen Sie für den Server einen DynDNS-Dienst, damit er auch bei wechselnder (dynamischer) IP-Adresse stets erreichbar bleibt.

Die Verschlüsselung von Mumble arbeitet mit AES und 128 Bit, was für diesen Zweck als ausreichend angesehen werden kann. Weitere Informationen zu Mumble finden Sie im Wiki zu diesem Projekt (*http://wiki.mumble.info*).

10 ANONYMES SURFEN

Der Datensammelwut im Internet sind fast keine Grenzen gesetzt. Besonders umfangreich fallen natürlich die Datenbestände bei den großen Internetkonzernen wie Google, Apple oder Microsoft aus, die durch ihre vielen Angebote auch das Nutzerverhalten detailliert beobachten können. Auf sozialen Netzwerken hinterlassen Nutzer von sich aus umfangreiche Informationen, und die großen Werbevermarkter sammeln Unmengen von Daten, um immer mehr über das Surfverhalten herauszubekommen. Wenn Sie Gratisdienste nutzen, sollten Sie sich keinen Illusionen hingeben, denn wenn Sie auch kein Geld ausgeben, so zahlen Sie in den meisten Fällen letztlich doch, indem Sie den Konzernen Ihre Daten zur Verfügung stellen. Zudem gibt es die nicht unberechtigte Angst vor staatlichen Überwachungsaktivitäten und Datensammlungen, denn auch Geheimdienste und Strafverfolger sind in dieser Hinsicht überaus aktiv, wie die Enthüllungen rund um die Snowden-Affäre eindrucksvoll belegen.

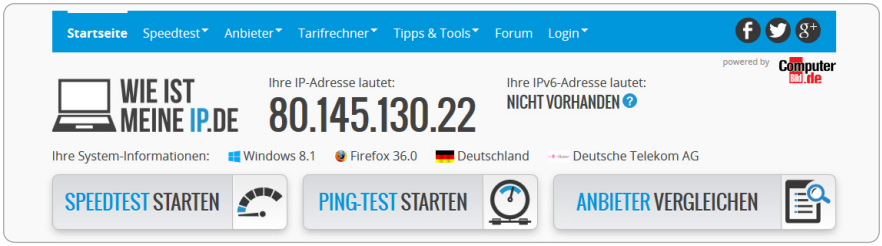
10.1 Wie viel Anonymität darf sein?

Schon seit Langem wird um die Möglichkeit zur anonymen Nutzung des Internets gestritten. Die Gegner verweisen auf die Missbrauchspotenziale einer weitgehend anonymen und unkontrollierten Nutzung, die von vergleichsweise moderaten Fällen wie Beschimpfungen oder Beleidigungen in Onlineforen über illegale Downloads von Filmen und Musik oder Software bis zu schwerer Kriminalität wie der Verbreitung von Kinderpornografie oder terroristischer Propaganda reicht. Die Nutzung zuverlässig verschlüsselter Informationskanäle wird von vielen Skeptikern daher kritisch gesehen, und Forderungen nach einer Einschränkung einer umfassenden Ende-zu-Ende-Verschlüsselung werden in der Politik immer lauter.

Dagegen stehen die Argumente von Datenschützern und Bürgerrechtlern, denen derartige Forderungen nach einer weitgehenden Abschaffung anonymer Nutzungsmöglichkeiten viel zu weit gehen. Man verweist darauf, dass jeder Anwender das Recht hat, seine persönlichen Daten im Internet zu schützen und die zahlreichen Daten sammelnden Einrichtungen vom Zugriff auf diese Informationen auszuschließen.

Erkennungsmerkmal IP-Adresse

Mit der Anonymität im Internet ist es für den Normalanwender ohnehin nicht so weit her, wie man vielleicht denkt, denn jeder mit dem Internet verbundene Rechner benötigt eine eindeutige Adresse, damit der Datenaustausch überhaupt stattfinden kann. Und üblicherweise speichern Webserver die IP-Adressen der Besucher. Die meisten Nutzer verwenden zwar keine festen IP-Adressen, sodass kein direkter Rückschluss auf die Anschlussinhaber möglich ist, allerdings lassen sich diese Informationen über die Provider ermitteln, bei denen die IP-Adressen für die jeweiligen Anschlüsse vergeben werden.



Über Webseiten wie *www.wieistmeineip.de* können Sie Ihre aktuelle IP-Adresse abrufen.

Um genau diese Daten geht es auch in der Diskussion um die Vorratsdatenspeicherung, denn über die Aufzeichnungen bei den Providern kann auch nachträglich festgestellt werden, von welchem Internetanschluss zu welchen Zeiten welche Verbindungen genutzt wurden. Nach dem weitgehenden Verbot dieser verdachtsunabhängigen Vorratsdatenspeicherung durch das Bundesverfassungsgericht speichern die meisten Provider derzeit die Verbindungsdaten hierzulande nur wenige Wochen, sodass auch Polizei und Strafverfolger nur einen engen Spielraum haben, um Ermittlungen zu führen.

IP-Adresse und mehr

Die IP-Adresse verrät bei der Kommunikation mit Webservern schon einiges über den Nutzer. So ist erkennbar, welchen Provider der Teilnehmer nutzt, und auch der ungefähre Standort ist zu sehen. Die Standortdaten werden häufig verwendet, was viele deutsche Internetnutzer auf YouTube erfahren haben, wenn Videos aufgrund von Streitigkeiten mit Verwertungsgesellschaften

gesperrt waren, während dieselben Videos in anderen Ländern frei verfügbar sind. Erkennt der YouTube-Server anhand der IP-Adresse, dass Sie die Seite von Deutschland aus abrufen, können Sie die gesperrten Inhalte nicht sehen. Im Fall von YouTube mag dies zwar ärgerlich, aber noch hinnehmbar sein, in anderen Ländern werden auf ähnliche Weise aber weite Teile des Webs zensiert und unzugänglich gemacht.

PROXIES ZUM VERSCHLEIERN DER IP-ADRESSE

Um derartige Einschränkungen zu umgehen, gibt es einige recht simple Verfahren, mit denen Webserver getäuscht werden. Das Prinzip ist einfach. Statt einer direkten Verbindung zum gewünschten Webserver wird eine Umleitung über einen anderen Rechner genommen. Dieser andere Rechner ist ein Stellvertreter, der die Verbindung zum eigentlich gewünschten Server herstellt. Der bekommt dann nur die IP-Adresse des Stellvertreters zu sehen. Im YouTube-Beispiel sieht der YouTube-Server etwa eine amerikanische IP-Adresse und liefert das gewünschte Video aus. Über diesen Stellvertreter können Sie auch in Deutschland in den Genuss des Videos gelangen. Derartige Lösungen werden als Proxyserver (engl. für Stellvertreter) bezeichnet.

Allerdings müssen auch Proxyserver darüber Buch führen, welche Ursprungs-IP welche Zieladressen aufruft. Und üblicherweise werden diese Daten über einen gewissen Zeitraum gespeichert, sodass Nutzer prinzipiell auch im Nachhinein identifiziert werden können. Wie lange diese Daten gespeichert werden, hängt von den Vorschriften am Standort des Proxyanbieters ab. Zur Verschleierung illegaler Aktivitäten taugen Proxies daher nicht. Zudem müssen die Nutzer den Betreibern der Proxies auch generell vertrauen, denn diese könnten deren Aktivitäten natürlich ebenfalls überwachen.

Neben der IP-Adresse übermittelt der Browser beim Surfen im Web auch noch einige weitere Informationen. So identifiziert er sich selbst und nennt dabei auch das verwendete Betriebssystem. Diese Daten werden beim Webserver beispielsweise dazu verwendet, die Webseiten automatisch in einer für diese Plattform optimierten Form zu präsentieren.

Cookies

Neben den IP-Adressen gibt es verschiedene andere Möglichkeiten, Nutzer auf Webseiten wiederzuerkennen oder sogar zu identifizieren. Dabei setzen die Betreiber von Webdiensten und Websites oder auch spezialisierte Werbedienstleister unterschiedliche Methoden ein, um Webseitenbesucher wiederzuerkennen oder personalisierte Werbebanner anzubieten.

Die bekannteste Technik dieser Art sind Cookies. Dabei handelt es sich um kleine Textdateien, über die Daten auf dem Rechner des Nutzers gespeichert und vom Webserver ausgelesen werden können. Die Einsatzmöglichkeiten für Cookies sind sehr vielfältig. So sind sie einerseits völlig unbedenklich und nützlich, wenn sie etwa das Wiedererkennen eines Nutzers ermöglichen und diesem dadurch eine erneute Anmeldung auf einer Seite ersparen. Auch Seiten mit personalisierten Inhalten lassen sich hierüber direkt ohne umständliche Eingabe eines Nutzernamens abrufen, und Warenkorbsysteme in Onlineshops werden ebenfalls so realisiert.

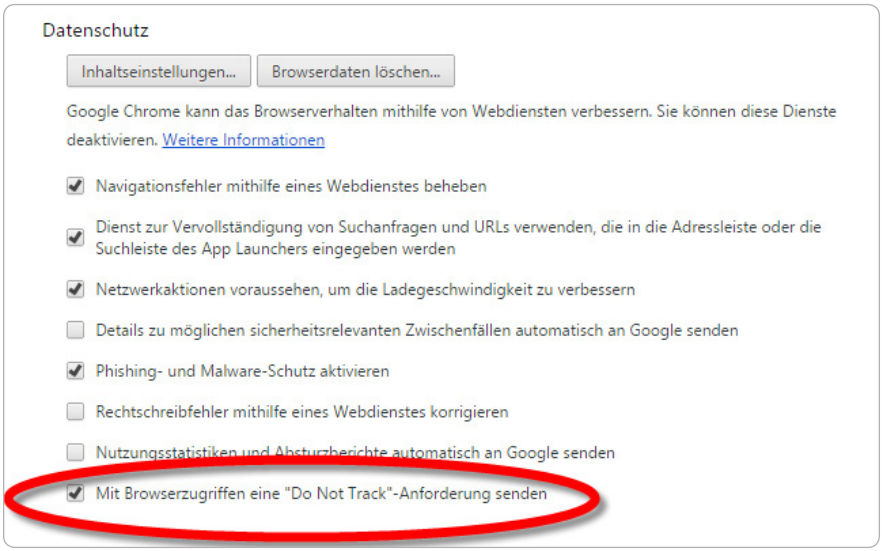
Viele Websites weisen die Besucher auf den Einsatz von Cookies hin.

Cookies können aber auch für eher unschöne Zwecke verwendet werden. Bedenklich sind vor allem Cookies, mit denen Ihr Surfverhalten ausspioniert werden kann. Besonders für Werbevermarkter sind diese Informationen von Interesse, denn wenn das Nutzerverhalten bekannt ist, können Nutzern passgenaue Werbebanner eingeblendet werden, die für Werbetreibende natürlich von besonderem Wert sind und für die ein entsprechend hoher Preis gezahlt wird.

NICHT ALLE COOKIES AKZEPTIEREN

Konventionelle Cookies lassen sich über den Browser verwalten. Datenschützer und Sicherheitsexperten raten zu eher restriktiven Vorgaben, denn je weniger Cookies Sie auf Ihrem Rechner zulassen, desto geringer ist die Gefahr, dass darunter auch unerwünschte Varianten sind.

In Kapitel 3 dieses Buchs haben wie Ihnen bereits einige Tipps zu den Cookie-Einstellungen der verschiedenen Browser gegeben.



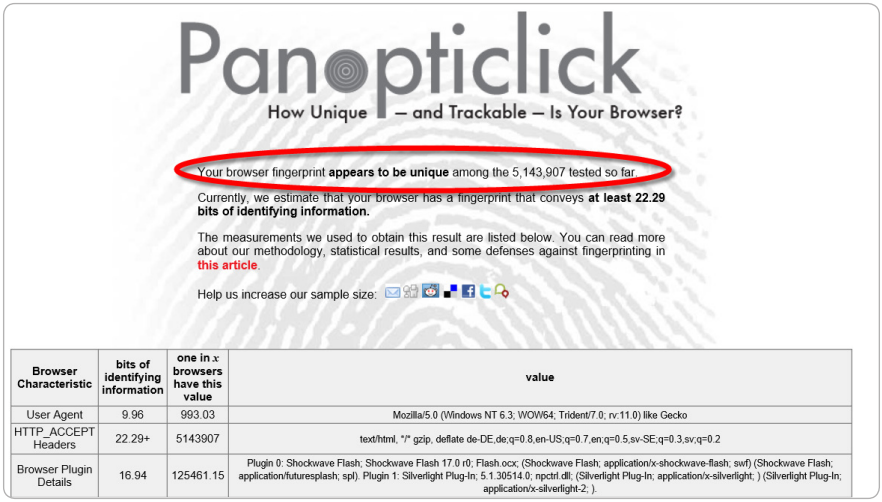
Die Do-not-Track-Option, hier im Chrome-Browser, soll eine unerwünschte Überwachung verhindern.

Fortgeschrittene Cookies und andere Tracking-Optionen

Längst gibt es neben einfachen Cookies auch andere Möglichkeiten zur Wiedererkennung von Nutzern bzw. Rechnern. Evercookies kombinieren etwa unterschiedliche Techniken, wie Flash- und Silverlight-Cookies, mit weiteren Merkmalen. Diese Cookies können nicht mehr so einfach gelöscht werden, sondern rekonstruieren sich selbstständig.

Zu diesen neuen Techniken gehört auch das »Canvas-Fingerprinting«, das sich den Umstand zunutze macht, dass verschiedene Rechner je nach Betriebssystem, Grafikkarte und -treiber, Browser und installierten Fonts den Text einer Webseite jeweils etwas unterschiedlich darstellen. Über diese Unterschiede lässt sich der Nutzer, genauer gesagt die genutzte Hardware, mit sehr hoher Sicherheit wiedererkennen. Zur Übermittlung übertragen die Webserver einen versteckten Text. Angewendet wird diese Technik von den Werbenetz-

werken Ligatus und AddThis. In einer Studie der Princeton-Universität wurde der Einsatz des Canvas-Fingerprintings vor einigen Jahren bereits auf über 5 Prozent von 100.000 getesteten Webseiten festgestellt.



Browser Characteristic	bits of identifying information	one in x browsers have this value	value
User Agent	9.96	993.03	Mozilla/5.0 (Windows NT 6.3; WOW64; Trident/7.0; rv:11.0) like Gecko
HTTP_ACCEPT Headers	22.29+	5143907	text/html, */* gzip, deflate de-DE,de;q=0.8,en-US;q=0.7,en;q=0.5,sv-SE;q=0.3,sv;q=0.2
Browser Plugin Details	16.94	125461.15	Plugin 0: Shockwave Flash; Shockwave Flash 17.0 r0; Flash.ocx; (Shockwave Flash; application/x-shockwave-flash; swf) (Shockwave Flash; application/futuresplash; spl). Plugin 1: Silverlight Plug-In; 5.1.30514.0; npctrl.dll; (Silverlight Plug-In; application/x-silverlight;) (Silverlight Plug-In; application/x-silverlight-2;).

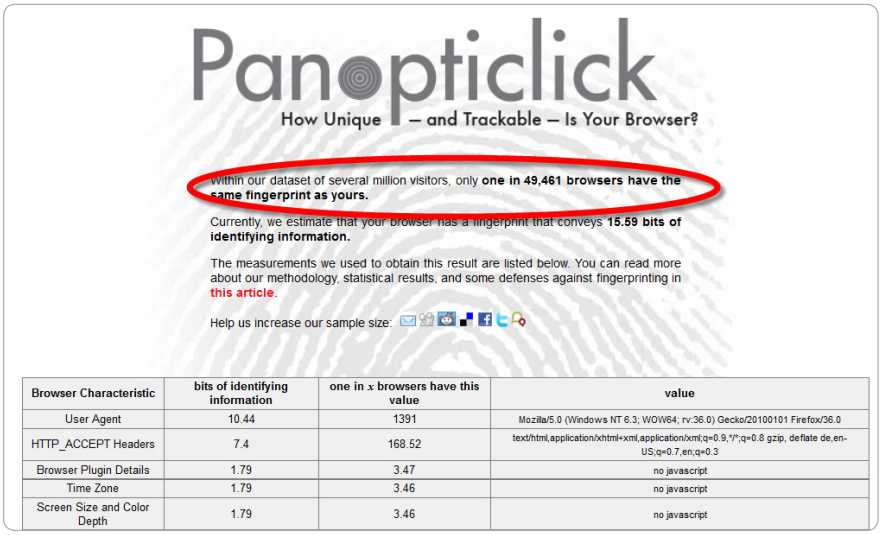
Viele Rechner sind über den Fingerabdruck eindeutig zu identifizieren.

Wie viele Daten über Ihre Hard- und Software über derartige Techniken abgefragt werden und wie einfach Sie wiedererkennbar sind, können Sie herausfinden, indem Sie die Testseite Panopticlick der EFF (*https://panopticlick.eff.org/*)

OHNE JAVASCRIPT SURFEN SIE ANONYMER

Einen gewissen Schutz vor dem Canvas-Fingerprinting und ähnlichen Tracking-Methoden kann Ihnen das Deaktivieren von JavaScript bieten, da die Daten meist über JavaScript-Techniken übermittelt werden. Mit abgeschaltetem JavaScript können wesentlich weniger Merkmale festgestellt werden, was eine eindeutige Identifizierung erschwert. Auch aus diesem Grund kann ein Einsatz von Tools zum gezielten Blockieren bestimmter Skripte angeraten sein. Ein völliges Deaktivieren von JavaScript ist dagegen nicht sinnvoll, da dadurch fast alle Webseiten nur noch eingeschränkt oder gar nicht mehr nutzbar sind.

aufrufen und den Test starten. Das Ergebnis zeigt Ihnen nicht nur, welche Daten abgefragt werden konnten, sondern auch, wie einzigartig das ermittelte Profil ist. Je nach Hard- und Software ist Ihr Rechner vielleicht komplett einzigartig oder zumindest relativ gut identifizierbar, wenn nur vergleichsweise wenige Systeme die gleichen Daten aufweisen.



Browser Characteristic	bits of identifying information	one in *x* browsers have this value	value
User Agent	10.44	1391	Mozilla/5.0 (Windows NT 6.3; WOW64; rv:36.0) Gecko/20100101 Firefox/36.0
HTTP_ACCEPT Headers	7.4	168.52	text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 gzip, deflate de,en-US;q=0.7,en;q=0.3
Browser Plugin Details	1.79	3.47	no javascript
Time Zone	1.79	3.46	no javascript
Screen Size and Color Depth	1.79	3.46	no javascript

Mit abgeschaltetem JavaScript sind Sie immerhin nicht mehr ganz so eindeutig zu identifizieren.

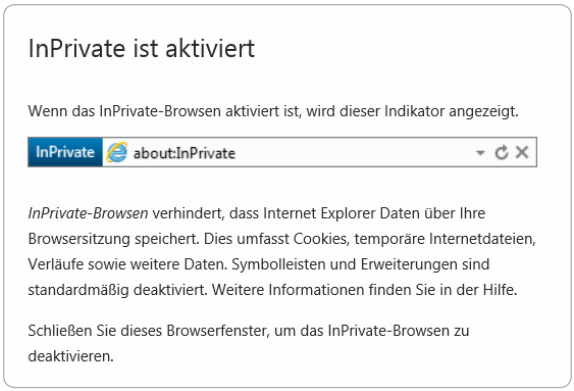
10.2 Optionen für mehr Anonymität

Für etwas mehr Anonymität können Sie beim Surfen relativ einfach sorgen. Die simpelste Methode ist die in allen Browsern integrierte Option zum privaten Surfen. Allerdings sind die Auswirkungen dieser Funktion gering und beschränken sich vor allem auf Datenspuren auf dem eigenen Rechner. Andere Methoden wie die Nutzung von Anonymisierungsproxies oder VPN-Servern sind aufwendiger, mit ihnen hinterlassen Sie aber auch deutlich weniger Spuren im Internet. Zudem verhelfen Browsererweiterungen zu etwas mehr Anonymität, und schließlich können Sie durch die Nutzung von Diensten, die auf das Sammeln von Daten weitgehend verzichten, dazu beitragen, dass wissbegierige Anbieter nicht allzu viele Daten über Sie bekommen.

Browseroption zum privaten Surfen

Das »private Surfen« ist eine Option, die alle großen Browser bieten. Die erzielbare Privatheit bezieht sich allerdings weitestgehend auf die Daten, die auf Ihrem Rechner gespeichert werden. Wenn Sie in diesem Modus surfen, werden die besuchten Webadressen nicht im Browserverlauf gespeichert, sodass andere Nutzer mit Zugang zu Ihrem Rechner nicht mehr sehen können, welche Websites Sie besucht haben.

Ebenso werden die im Browsercache zwischengespeicherten Dateien gelöscht und Cookies entweder komplett abgelehnt oder spätestens bei Beendigung dieses Modus wieder gelöscht, womit dann keine Spuren direkt auf dem Rechner mehr vorhanden sind. Außerhalb Ihres eigenen Rechners sind Sie dagegen keineswegs anonym unterwegs. Auf den Webservern wird Ihre IP-Adresse ganz normal erfasst, und auch Ihr Provider weiß genau, welche Seiten Sie aufgerufen haben.



Der Internet Explorer listet auf, was beim InPrivate-Modus gelöscht bzw. blockiert wird.

PRIVATES SURFEN AKTIVIEREN

Beim Firefox starten Sie das private Surfen über den Menüpunkt *Privates Fenster*. Sie können auch Links mit der rechten Maustaste anklicken und im Kontextmenü die Option zum Öffnen im privaten Fenster auswählen. Im Internet Explorer führt der Weg über die *Extras/Sicherheit/InPrivate-Browsen*. Bei Chrome starten Sie diesen Modus über den Menüeintrag *Neues Inkognito-Fenster*.

INDEX

Symbole

A

B

C

W

X

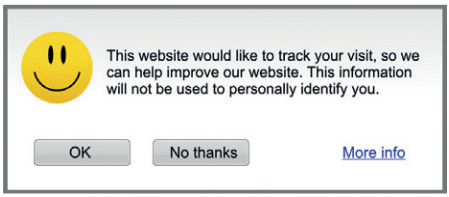
Z

SCHNELLEINSTIEG
SICHER SURFEN IM WEB

ABZOCKE IM INTERNET? NICHT MIT MIR!

„Checklisten und Sicherheitstipps – entspannt Surfen“

Computerviren und Würmer, die weltweit Millionen von PCs befallen und lahmlegen, wie es Melissa und dem I-Love-You-Virus vor 15 Jahren gelang, gibt es heute nicht mehr. Das darf jedoch keineswegs als Entwarnung verstanden werden – ganz im Gegenteil! Es gibt neue Gefahren, die sogar noch gravierendere Folgen haben können.



Erprobte Sicherheitskonzepte für entspanntes Surfen, am Beispiel realer Betrügereien vorgestellt
(Quelle: Screenshots silktide.com, paypal.de)

Lassen Sie sich den Spaß am Internet nicht verderben ...
Auch wenn die Aufzählung der potenziellen Gefahren auf den ersten Blick recht abschreckend wirkt, müssen Sie nicht gleich in Panik geraten und auf die Internetnutzung verzichten. Zum Glück gibt es zahlreiche Möglichkeiten, die Risiken so weit zu verringern, dass Sie sich weiterhin weitgehend unbeschwert im Internet bewegen und von den vielfältigen Nutzungsmöglichkeiten profitieren können.

... werden Sie aktiv, handeln Sie und geben Sie Betrügern keine Chance
Dieses Buch ist Ihr Schild gegen Botnetzte und Zombie-Rechner, gegen Betrügereien beim Onlinebanking, gegen Identitätsdiebstahl, gegen unerwünschte Überwachung und Datenweitergabe – Ihr Schild gegen den alltäglichen Betrug. Sicherheit beim Surfen stellt sich nicht von allein ein. Sie müssen selbst aktiv werden! Dabei ist es nicht mit einer einmaligen Aktion wie der Installation eines Antivirenprogramms getan, sondern Sie sind dauerhaft gefordert, aufmerksam zu bleiben und vorsichtig zu handeln. Dieses Buch hilft Ihnen dabei.

Aus dem Inhalt:

9 783645 603973